

JP5224604A DEVICE FOR MANAGING PUBLIC KEY CIPHER SYSTEM

Bibliography

DWPI Title

Cryptographic system using public key private key pairs generates two key pairs using one known and one unknown seed value with corresponding control vectors to control use of key pairs.

Original Title

DEVICE FOR MANAGING PUBLIC KEY CIPHER SYSTEM

Assignee/Applicant

Standardized: IBM

Original: INTERNATL BUSINESS MACH CORP <IBM>

Inventor

MATYAS STEPHEN M ; JOHNSON DONALD B ; LE AN V ; WILLIAM C MARTIN ; ROSTISLAW PRYMAK ; JOHN D WILKINS

Publication Date (Kind Code)

1993-09-03 (A)

Application Number / Date

JP1992231284A / 1992-08-06

Priority Number / Date / Country

US1991766533A / 1991-09-27 / US

JP1992231284A / 1992-08-06 / JP

Abstract

PURPOSE: To make a user port public and private keys from a certain cipher system to another cipher system and improve security protection, by generating a pair of the public key and the private key from a path phrase first.

CONSTITUTION: This device is provided with a cipher facility 30, a cipher key data set 32, a ciphering mechanism access program 24 and an application program 36. Then, the first pair of the public key and the private key is generated by using a first seed value known to the user and a first control vector for defining the first private use of the first pair of the public key and the private key is generated. Then, the second pair of the public key and the private key is generated by using a second seed value known to the user and a second control vector for defining the second private use of the second pair of the public key and the private key is generated. Then, the private use of the first pair of the public key and the private key is controlled by using the first control vector and the private use of the second pair of the public key and the private key is controlled by using the second control vector.

【特許請求の範囲】

【請求項1】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理する方法であって、ユーザに知られている第1のシード値を用いて第1の公用キー、私用キーペアを生成し、また前記第1の公用キー、私用キーペアの第1の使用を定義する第1の制御ベクトルを生成するステップと、ユーザに知られている第2のシード値を用いて第2の公用キー、私用キーペアを生成し、また前記第2の公用キー、私用キーペアの第2の使用を定義する第2の制御ベクトルを生成するステップと、前記第1の制御ベクトルを用いて前記第1の公用キー、私用キーペアの使用を制御するステップと、前記第2の制御ベクトルを用いて前記第2の公用キー、私用キーペアの使用を制御するステップとを含むことを特徴とする方法。

【請求項2】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理する方法であって、パスフレーズから導出される第1のシード値を用いて第1の乱数を生成するステップと、ユーザには知られない第2のシード値を用いて第2の乱数を生成するステップと、前記第1の乱数を用いて第1の公用キー、私用キーペアを生成し、また前記第1の公用キーおよび前記第1の私用キーの第1の使用を定義するために、それぞれ第1の公用キー制御ベクトルおよび第1の私用キー制御ベクトルを生成するステップと、前記第2の乱数を用いて第2の公用キー、私用キーペアを生成し、また前記第2の公用キーおよび前記第2の私用キーの第2の使用を定義するために、それぞれ第2の公用キー制御ベクトルおよび第2の私用キー制御ベクトルを生成するステップと、前記第1の公用キー制御ベクトルおよび前記第1の私用キー制御ベクトルを用いて、それぞれ前記第1の公用キーおよび前記第1の私用キーの使用を制御するステップと、前記第2の公用キー制御ベクトルおよび前記第2の私用キー制御ベクトルを用いて、それぞれ前記第2の公用キーおよび前記第2の私用キーの使用を制御するステップとを含むことを特徴とする方法。

【請求項3】データ処理システムにおいて、キー発生器を有する暗号システムを管理する方法であって、パスフレーズから導出される第1のシード値を用いて第1の乱数を生成するステップと、ユーザに知られない第2のシード値を用いて第2の乱数を生成するステップと、前記第1の乱数を用いて第1キーを生成し、また前記第1のキーの使用を制御するための第1の制御ベクトルを

生成するステップと、

前記第2の乱数を用いて第2のキーを生成し、また前記第2のキーの第2の私用を制御するための第2の制御ベクトルを生成するステップと、前記第1の制御ベクトルにより前記第1のキーの使用を制御するステップと、前記第2の制御ベクトルにより前記第2のキーの使用を制御するステップと、前記第1のキーの前記第1の使用が、前記第2のキーの前記第2の使用と異なるステップとを含むことを特徴とする方法。

【請求項4】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法であって、パスフレーズから導出される第1のシード値を用いて乱数を生成するステップと、前記乱数を用いて公用キー、私用キーペアを生成し、前記第1の制御ベクトルは前記公用キーの使用を制御するもので、前記第2の制御ベクトルは前記私用キーの使用を制御するものであり、前記公用キーに対して前記第1の制御ベクトルを生成し、また前記私用キーに対して前記第2の制御ベクトルを生成するためのステップを含むことを特徴とする方法。

【請求項5】データ処理システムにおいて、公用キー、私用キーペアを含む公用キー暗号システムを管理するための方法であって、パスフレーズから導出されるシード値を用いて乱数を生成するステップと、前記乱数を用いて公用キー、私用キーペアを生成するステップとを含むことを特徴とする方法。

【請求項6】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法であって、ユーザに知られている第1のシード値を用いて第1の公用キー、私用キーペアを生成し、また前記第1の公用キー、私用キーペアの第1の使用を定義する第1の制御ベクトルを生成するステップと、ユーザに知られない第2のシード値を用いて第2の公用キー、私用キーペアを生成し、また前記第2の公用キー、私用キーペアの第2の使用を定義する第2の制御ベクトルを生成するステップと、前記第1の制御ベクトルを用いて前記第1の公用キー、私用キーペアの使用を制御するステップと、前記第2の制御ベクトルにより前記第2の公用キー、私用キーペアの使用を制御するステップとを含む方法を実行することを特徴とする方法。

【請求項7】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法であって、パスフレーズから導出される第1のシード値を用いて第

1の乱数を生成するステップと、
ユーザに知られない第2のシード値を用いて第2の乱数を生成するステップと、
前記第1の乱数を用いて第1の公用キー、私用キーペアを生成し、また前記第1の公用キーおよび前記第1の私用キーの第1の使用をそれぞれ定義するための第1の公用制御キーベクトルおよび第2の私用キー制御ベクトルを生成するステップと、
前記第2の乱数を用いて第2の公用キー、私用キーペアを生成し、また前記第2の公用キーおよび前記第2の私用キーの第2の使用をそれぞれ定義するために、第2の公用キー制御ベクトルおよび第2の私用キー制御ベクトルを生成するステップと、
前記第1の公用キー制御ベクトルおよび前記第1の私用キー制御ベクトルを使用して、それぞれ前記第1の公用キーおよび前記第1の私用キーの前記第1の使用を制御するステップと、
前記第2の公用キー制御ベクトルおよび前記第2の私用キー制御ベクトルを使用して、それぞれ前記第2の公用キーおよび前記第2の私用キーの使用を制御するステップとを含むことを特徴とする方法。
【請求項8】データ処理システムにおいて、キー発生器を有する暗号システムを管理するための方法であって、パスフレーズから導出される第1のシード値を用いて第1の乱数を生成するステップと、ユーザに知られない第2のシード値を用いて第2の乱数を生成するステップと、前記第1の乱数を用いて第1のキーを生成し、また前記第1のキーの使用を制御するための第1の制御ベクトルを生成するステップと、前記第2の乱数を用いて第2のキーを生成し、また前記第2のキーの第2の使用を制御するための第2の制御ベクトルを生成するステップと、前記第1の制御ベクトルにより前記第1のキーの使用を制御するステップと、前記第2の制御ベクトルにより前記第2のキーの使用を制御するステップと、前記第1のキーの第1の使用が前記第2のキーの前記第2の使用とは異なっているステップとを含むことを特徴とする方法。
【請求項9】データ処理システムにおいて、公用キー、私用キーペアを含む公用キー暗号システムを管理するための方法であって、パスフレーズから導出される第1のシード値を用いて乱数を生成するステップと、前記乱数を用いて公用キー、私用キーペアを生成し、また前記公用キーに対する第1の制御ベクトルおよび前記私用キーに対する第2の制御ベクトルを生成し、前記第1の制御ベクトルが前記公用キーの使用を制御し、前記第2の制御ベクトルが前記私用キーの使用を制御するス

テップとを含むことを特徴とする方法。

【請求項10】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法であって、パスフレーズから導出されるシード値を用いて乱数を生成するステップと、前記乱数を用いて公用キー、私用キーペアを生成するステップとを含むことを特徴とする方法。

【請求項11】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、ユーザに知られる第1シード値を用いて第1公用キー、私用キーペアを生成し、また前記第1公用キー、私用キーペアの第1使用を定義する第1制御ベクトルを生成する第1生成手段と、ユーザに知られない第2シード値を用いて第2公用キー、私用キーペアを生成し、また前記第2公用キー、私用キーペアの第2使用を定義する第2制御ベクトルを生成する第2生成手段と、前記第1制御ベクトルを用いて前記第1公用キー、私用キーペアの使用を制御するための、前記第1生成手段に連結される制御手段と、前記第2制御ベクトルにより前記第2公用キー、私用キーペアの使用を制御するための、前記第2生成手段に連結される前記制御手段とを含むことを特徴とする装置。

【請求項12】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、パスフレーズから導出される第1シード値を用いて第1乱数を生成するための第1生成手段と、ユーザに知られない第2シード値を用いて第2乱数を生成するための第2生成手段と、前記第1乱数を用いて第1公用キー、私用キーペアを生成し、また前記第1公用キーおよび前記第1私用キーの第1使用をそれぞれ定義するための第1公用キー制御ベクトルおよび第1私用キー制御ベクトルを生成する前記第1生成手段と、前記第2乱数を用いて第2公用キー、私用キーペアを生成し、また前記第2公用キーおよび前記第2私用キーの第2使用をそれぞれ定義するための第2公用キー制御ベクトルおよび第2私用キー制御ベクトルを生成する前記第2生成手段と、前記第1公用キー制御ベクトルおよび前記第1私用キー制御ベクトルをそれぞれ用いて、前記第1公用キーおよび前記第1私用キーの使用を制御するための、前記第1生成手段に連結される制御手段と、前記第2公用キー制御ベクトルおよび前記第2私用キー制御ベクトルをそれぞれ用いて、前記第2公用キーおよび前記第2私用キーの使用を制御するための、前記第2生成手段に連結される制御手段とを含むことを特徴とする

る装置。

【請求項13】データ処理システムにおいて、キー発生器を有する暗号システムを管理するための装置であって、
パスフレーズから導出される第1シード値を用いて第1乱数を生成するための第1生成手段と、
ユーザに知られない第2シード値を用いて第2乱数を生成するための第2生成手段と、
前記第1乱数を用いて第1キーを生成し、また前記第1キーの使用を制御するための第1制御ベクトルを生成する前記第1生成手段と、
前記第2乱数を用いて第2キーを生成し、また前記第2キーの第2使用を制御するための第2制御ベクトルを生成する前記第2生成手段と、
前記第1制御ベクトルでもって前記第1キーの使用を制御するための前記第1生成手段に連結される制御手段と、
前記第2制御ベクトルでもって前記第2キーの使用を制御するための前記第2生成手段に連結される前記制御手段と、
前記第1キーの前記第1使用が前記第2キーの前記第2使用と異なることを含むことを特徴とする装置。

【請求項14】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
パスフレーズから導出される第1シード値を用いて乱数を生成する生成手段と、
前記乱数を用いて公用キー、私用キーペアを生成し、また前記公用キーに対する第1制御ベクトルおよび前記私用キーに対する第2制御ベクトルを生成し、前記第1制御ベクトルが前記公用キーの使用を制御し、前記第2制御ベクトルが前記私用キーの使用を制御する前記生成手段とを含むことを特徴とする装置。

【請求項15】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
パスフレーズから導出されるシード値を用いて乱数を生成する生成手段と、
前記乱数を用いて公用キー、私用キーペアを生成する前記生成手段とを含むことを特徴とする装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、広くはデータ処理のシステムと方法、更に詳しくは機密保護を高めるためデータ処理システムに於て使用する暗号システムおよび方法に関する。

【0002】

【従来の技術およびその課題】以下の特許および同時系属出願の特許明細書は本発明に関連し参考としてここに記載する。

【0003】B.Brachtl 等の「生成ステーション設定制御値を経由する暗号キーの制御的使用」USP 4, 850, 017 (1989年7月18日、譲受人 IBM Corporation)

S.M. Matyas 等の「制御ベクトルを用いるキーの機密保護管理」USP 4, 941, 176 (1990年7月10日、譲受人 IBM Corporation)

S.M. Matyas 等の「制御ベクトルを用いるデータ暗号演算」USP 4, 918, 728 (1990年4月17日、譲受人 IBM Corporation)

S.M. Matyas 等の「制御ベクトルを用いる個人識別番号処理」USP 4, 924, 514 (1990年5月8日、譲受人 IBM Corporation)

S.M. Matyas 等の「拡張制御キーを用いるキーの機密保護管理」USP 4, 924, 515 (1990年5月8日、譲受人 IBM Corporation)

S.M. Matyas 等の「制御ベクトル変換を用いる機密保護キー管理」USP 4, 993, 069 (1991年2月12日、譲受人 IBM Corporation)

S.M. Matyas 等の「プログラム可能な制御ベクトル検査を用いる機密保護キー管理」USP 5, 007, 089 (1991年4月9日、譲受人 IBM Corporation)

B.Brachtl 等の「公用一方向暗号化機能に基く修正検出コードを用いるデータ認証」USP 4, 908, 861 (1990年3月3日、譲受人 IBM Corporation)

D.Abraham 等「外部プログラム能力を有するスマートカードおよび同じくつくる方法」出願番号004, 501 (1987年1月19日ファイル、譲受人 IBM Corporation)

S.M. Matyas 等の「RSA暗号変数記憶装置を圧縮する手法」USP 4, 736, 423 (1988年4月5日、譲受人 IBM Corporation)

S.Schulzの「乱数発生器回路」USP 4, 905, 176 (1990年2月27日、譲受人 IBM Corporation)

S.M. Matyas 等の「多重パス検査により制御ベクトルを用いるキーの機密保護管理」出願番号07/596, 637 (1990年10月12日ファイル、譲受人 IBM Corporation)

S.M. Matyas 等の「制御ベクトル実施の代替モードを用いる安全な暗号演算」出願番号07/574, 012 (1990年8月22日ファイル、譲受人 IBM Corporation)

S.M. Matyas 等の「キーに対するインポート完全性レベルに基き、公用キーの使用を制御する方法および装置」出願番号07/602, 989 (1990年10月24日ファイル、譲受人 IBM Corporation)

S.M. Matyas 等の「制御ベクトルに基づくハイブリッド

公用キーアルゴリズム／データ暗号化アルゴリズムキー分散法」出願番号 07/748,407 (1991年8月22日ファイル、譲受人 IBM Corporation) S.M. Matyas 等の「制御ベクトルに基づく公用キー暗号システムキー管理」(本特許出願と同日出願、譲受人 IBM Corporation)

引用したS.M. Matyas 等による特許に述べられている暗号体系は暗号キーとキーの創案者が意図するキーの使用に対し認証を与える制御ベクトルとの連繫に基づいている。S.M. Matyas 等による引用特許に述べられている暗号体系はデータ暗号化アルゴリズム(DEA)(米国標準規格×3.92-1981、データ暗号化アルゴリズム、米国標準規格協会、New York(1981年12月31日)参照)に基づいているのに対し、本発明はDEA等の機密キーと公用キーアルゴリズムの両方に基づいている。本発明に従って、各種キー管理機能、データ暗号機能、その他データ処理機能が制御ベクトルを用いて可能である。システム管理者は本発明に従う適当な制御ベクトルを選択することにより、その機密保護方針の実施に当って柔軟性を発揮することが出来る。暗号体系中の暗号ファシリティ(CF)は前に引用したS.M. Matyas 等の特許中に述べられている。CFは暗号命令の集合に対する命令処理装置であって、暗号化方法およびキー生成方法を実行する。暗号ファシリティにおける記憶装置が内部暗号変数の集合を記憶する。各暗号命令は入力パラメータの集合を出力パラメータの集合に変換するのに必要な一連の処理ステップに関し述べられている。暗号ファシリティアプリケーションプログラム(CFAP)もまた参照された特許および出願明細書中に述べられており、これは対応する入力および出力パラメータと共に命令略号およびアドレスからなる各暗号命令に対する呼び出し方法を(呼び出し順序として)定義する。

【0004】公用キー暗号化アルゴリズムはW.Diffie、M.E.Hellman 共著の「プライバシーと認証：暗号入門“Privacy and Authentication:An Introduction to Cryptography”」米国電気電子学会誌(IEEE)、67巻3号、1979年3月、pp.397~427に述べられている。公用キーシステムは、機密分散チャネルが充分な完全性レベルを有する限り、そのチャネルなしですますことを基にしている。公用キー暗号システムでは、2種のキーが使用され、その1は暗号化用であり他の1は解読用である。公用キーアルゴリズムは(1)インバースキーPU(暗号化用)およびPR(解読用)の無作為ペアを生成するのが容易であり、(2)PU、PRによる演算が容易であるが、(3)PUからPRを計算することは計算上は実行不可能であるように設計されている。ユーザは解読変換PRを機密に保ち、暗号化変換PUは、それを公用辞書におくことで公用する。誰でもメッセージを暗号化してそれをユーザに送信できるが、他の誰も彼に向けられたメッセージを解読は出来ない。PUでも

って暗号化し、PRでもって解読することが可能であり、屢々望まれる。この理由で、PUは一般に公用キーと呼ばれ、PRを一般に私用キーと呼ぶ。公用キー暗号システムの系特徴はメッセージの送信者を独特に識別するデジタル署名を提供することである。もしユーザAが署名ずみのメッセージMをユーザBに送信しようと思うと、彼は彼の私用キーPRでその上に操作し、署名ずみメッセージSを作成する。PRは機密が望ましい時はAの解読キーとして用いられたが、ここでは彼の「暗号化」キーとして用いる。ユーザBがメッセージSを受信すると、彼はAの公用PUでもって暗号文Sに操作してメッセージMを回復できる。Aのメッセージを連続的に解読することにより、受信者Bはそれが送信者Aから来たという確証を得る。公用キー暗号の例は次の米国特許、Hellman 等のUSP 4,218,582「公用キー暗号装置および方法」、Hellman 等のUSP 4,200,770「暗号装置および方法」、Rivest等のUSP 4,405,829「暗号通信システムおよび方法」に与えられている。

【0005】たいていの暗号システムにおいては、一旦暗号キーが生成されると、暗号キーデータセットの中に暗号化した形で記憶することが出来るし、または生成装置から受信装置に暗号化した形で伝送し、そこで受信装置での記憶および使用に適当な形に再暗号化することも出来る。適当な媒体(例えばディスク、磁気テープ、メモリカード、スマートカード)にキーを書き込み、その媒体を移送することにより、またはキーを電子的に伝送することによりある装置から他の装置にキーはポートされる。しかし、移送または伝送されているキーが対称キー暗号化アルゴリズム(例：データ暗号化アルゴリズム)と共に用いられる機密キーのような機密キーであるか、または非対称キー暗号アルゴリズムと共に用いる公用および私用キーペアの私用キーである時には、キーが敵により傍受されるかも知れない危険が常に存在する。機密または私用キーを安全に移送または伝送する一つの方法は、送信装置と受信装置間で共有するキーで、それらを暗号化することである。しかし、送信、受信装置がかかる機密保護暗号化チャネルを容易にするであろうキーを共有していない場合、または送信、受信装置がかかる機密保護チャネルを容易化するためにかかるキーイング関係を設定するのが不便あるいは不可能な場合がある。従って機密キーをある装置から他の装置にポートする唯一の便利な方法はクリアキーをポートすることしかないことがたびたびある。

【0006】

【課題を解決するための手段】

本発明の目的

本発明の目的は、ユーザが公用および私用キーをある暗号システムから別の暗号システムにポートする改良された方法を提供することにある。

【0007】本発明の別の目的はディスク、磁気テープ、メモリカード、またはスマートカード等の分離した記憶媒体を必要とすることなく、ユーザがある暗号システムから別の暗号システムに公用および私用キーをポートすることが出来るようにすることにある。

【0008】本発明の更に別の目的はユーザの公用および私用キーを生成し、ユーザが暗号装置を実際に使用中の期間に使用することができ、また、ユーザが暗号装置を不使用中はそのキーを暗号装置からページすることが出来るようにすることにある。

【0009】本発明の更に別の目的はユーザが暗号サービスを必要とする期間中は暗号能力を有するポータブルコンピュータ内で、ユーザの公用および私用キーを初期化し、また暗号システムが必要とされない時はそのキーをポータブルコンピュータからページさせることにある。

【0010】本発明の更に別の目的はパスフレーズ等のユーザが記憶している事柄だけから、ユーザの公用および私用キーペアを暗号装置ネットワーク内のいかなる暗号装置においても生成または再生成できる方法を提供することにある。

【0011】本発明の更に別の目的はパスフレーズ組合わせ数が2の128べき乗よりも大きく、なおそのパスフレーズがユーザが容易にそれを記憶できるような充分な冗長性を有することを保証するパスフレーズの構成法を提供することにある。

【0012】本発明の更に別の目的はキー生成アルゴリズムがRivest-Shamir-Adelman (RSA) 公用キー暗号アルゴリズムに基づいているところで、入力パスフレーズから公用キーペアおよび私用キーペアを生成および再生成するための方法を提供することにある。

【0013】本発明の更に別の目的はキー生成アルゴリズムがいかなる公用キー暗号アルゴリズムに基づいているところでも、入力パスフレーズから公用キーおよび私用キーペアを生成および再生成するための方法を提供することにある。

【0014】本発明の更に別の目的はキー生成アルゴリズムにパスフレーズに基づかない第1のタイプ、およびパスフレーズに基づく第2のタイプの公用キーおよび私用キーペアを作成させるキー管理システムを提供することにある。

【0015】本発明の別の目的はパスフレーズに基づかない第1のタイプの公用および私用キーペアには、第1のキー使用法が許されたキー使用法の第1の集合に基づくようにせしめ、またパスフレーズに基づく第2タイプの公用キーおよび私用キーペアには、第1のキー使用法が許されたキー使用法の第2の集合に基づくようにせしめるキー管理システムを提供することにある。

【0016】本発明の別の目的はパスフレーズから生成される公用キーおよび私用キーは、パスフレーズから生

成されない公用キーおよび私用キーとは暗号的に分離することができ、従ってパスフレーズから生成される公用キーおよび私用キーにより両タイプの生成される公用キーおよび私用キーを利用する暗号システムの全体機密保護を弱めることの起り得ないようなキー管理システムを提供することにある。

本発明の概要

上記その他の目的、特徴および効果はここに開示する本発明により達成される。本発明は暗号装置のネットワークにおいて、ある装置から他の装置に機密または公用キーをポートする代替手段を提供する。本発明はまた暗号装置のユーザが実際には暗号装置を使用していない間はその機密キーをページし、また実際に暗号装置を使用している間は機密キーを再生成するための手段を提供する。これはユーザによりキー生成アルゴリズムに提供されるパスフレーズから公用キーおよび私用キーペアを先づ生成することにより達成される。その後同じキーペアの再生成が必要になるたびに、ユーザは同じパスフレーズを入力し、それからキー生成アルゴリズムが同じ公用キーおよび私用キーペアを導出する。かかる手続きは暗号能力を有するポータブルのプログラマブルコンピュータ(PC)を所有する単一ユーザにより用いられる。ユーザが移動中はそのキーはシステムからページされる。ユーザが暗号システムを使用中は、そのキーは再生成される。パスフレーズも、例えば80文字以上と長いことがある点を除けば、考え方はパスワードと類似である。パスフレーズはより多くの文字を含みうるので、パスワードより多くの変異性を包含することができるが、ユーザがパスフレーズを記憶するのは容易である。

【0017】図1は装置を使用中は公用キーおよび私用キーを生成し、不使用中はそのキーをページしている2人のユーザ i 、 j により共有されている暗号システムAのブロック図を示したものである。ここで図1を参照し、時刻 t_1 に第1のユーザ(ユーザ i)は自己のパスフレーズを入力しキー生成機能呼び出すことにより自身の公用キーおよび私用キー PU_i 、 PR_i が暗号システムAに再生成されるようにする。時刻 t_0 から時刻 t_1 まで、ユーザ i は暗号キーを実際に使用する。時刻 t_1 にユーザ i はキーページ機能呼び出して、公用キーおよび私用キー PU_i 、 PR_i をページする。時刻 t_2 に、第2のユーザ(ユーザ j)が自己のパスワードを入力しキー生成機能呼び出すことにより、彼の公用キーおよび私用キー PU_j 、 PR_j が暗号システムAに再生成されるようにする。時刻 t_2 から時刻 t_3 まで、ユーザ j は実際に自己の暗号キーを使用する。時刻 t_3 に、ユーザ j はキーページ機能呼び出して自己の公用キーおよび私用キー PU_j 、 PR_j をページする。ここで述べるキーページ機能は公用キーおよび私用キーの両方ともページしている。現実には、私用キーのみをページすることで充分であろう。

【0018】図2は単一ユーザiがある装置使用を望むときは自己の公用キーおよび私用キーペアを生成し、その装置使用を終了すると自己のキーをページする単一ユーザiにより共用される暗号システムAおよびBのブロック図による説明である。こゝで図2を参照し、時刻t0に、ユーザiは自己のパスフレーズを入力しキー生成機能呼び出すことにより、自己の公用キーおよび私用キーPUi, PRiが暗号システムAに再生成されるようにする。時刻t0から時刻t1まで、ユーザiは実際に暗号キーを使用する。時刻t1に、ユーザiはキーページ機能呼び出すことにより、彼の公用キーおよび私用キーPUi, PRiをページする。時刻t1から時刻t2まで、ユーザは暗号システムAから暗号システムBに移動する。時刻t2に、ユーザiは自己のパスフレーズを入力し、キー生成機能呼び出すことにより自己の公用キーおよび私用キーPUi, RViが暗号システムBに再生成されるようにする。時刻t2から時刻t3までは、ユーザiは暗号キーを実際に使用する。時刻t3に、ユーザiはキーページ機能呼び出すことにより公用キーおよび私用キーPUi, RViをページする。

【0019】パスフレーズは自然言語例えば英語からとったワードまたはフレーズからなる。「時は風の如く、果実はバナナの如く飛ぶ」、「心配するな、悪いことなど起らない」、「父は弟に犬を買ってやった、弟はまだ子供だから」といったのがパスフレーズの例（必ずしも良い例ではないが）である。

【0020】パスフレーズは意味をもったワードの列であるから、たとえばパスフレーズが（空白を含み）80文字以上を含んでいたとしても、ユーザがそのパスフレーズで記憶し思い出すことが出来る。こういう訳で、パスフレーズ組合せの数は容易に2の128べき乗（すなわち倍長DEAキーの組合せ数以上）を越えることができる。ユーザにはパスフレーズを作るための命令の集合またはガイドラインも同時に提供する。これによりユーザが不注意により敵が容易に推測できるようなパスフレーズを使用することがないようにする。例えば「メアリーは小羊をもっていて…」といったパスフレーズは長くても、最初の2ワードを知られると、残りは分ってしまう。「ドナルドダック、ジャックベニィ、アルフレッド大王がゴルフボールを食べながらチェスをした」といったパスフレーズは敵が推測できないことは、これを読めば容易に理解できる。キー生成中、キーを生成する過程でキー生成アルゴリズムが用いる所要の乱数を生成するシード値として、パスフレーズが用いられる。パスフレーズから生成する乱数以外には、いかなる乱数をもキー生成アルゴリズムは使用しない。生成された公用キーおよび私用キーペア（PU, PR）はパスフレーズのみ依存するので同じキー生成アルゴリズムを実行する暗号装置ネットワークの中ならばどの暗号装置でも（PU, PR）を再生成できる。ネットワークが単一の販売会社

から購入した暗号装置から成立している場合、またはキー生成の方法が標準化されており、違う販売会社から入手する数種の製品に実行されている場合がこういった場合である。

【0021】

【実施例】暗号システムのユーザが与える文字列からキーを生成するという概念はIBM社情報保護システム（IPS）で実行してきたものであって、VM/CMSユーザガイド、Order No. SH20-2621, IBM Corporation（1982年8月）の情報保護システム暗号プログラムを参照された。この情報保護システムは、データファイルを暗号化したり解読したりするのに用いるキーを暗号システムのユーザが制御、管理するという概念に基いて設計されたファイル保護システムである。システム自身のキーは一切ない。データの暗号化または解読が必要となった時に、ユーザが暗号システムにキーを規定してやらなければならない。ユーザは16進数字キーまたは80文字までの文字列のいずれかを規定すればよい。文字列が入力された場合は、IPSは次の方法により入力文字列を56ビットキーに「クランチ」（なすわちハッシュ）する。入力文字列は80文字の長さに空白つき右側に埋込まれる。次に入力文字列は8文字のブロックに分割される。その結果の埋込データはその値がX「0101010101010101010101010101」である一定キーおよびその値がX「000000000000000000000000」である初期チューニング値を用い、暗号化ブロック連鎖（CBC）モードを用いてDEAで暗号される。最終64ビットブロックの暗号文の右端56ビットが「クランチ」データキー（パリティビットなし）として取り上げられる。

【0022】情報保護システムにおける文字列からデータキーを作成する方法は公用キーおよび私用キーペアの作成には拡張されない。公用キー生成アルゴリズムはより複雑なためである。ユーザが与えるパスフレーズから公用キーおよび私用キーペアを生成するためには、キー生成アルゴリズム自体を修正し、動的にシードされる擬似乱数発生器を使わなければならない。動的にシードされる擬似乱数発生器は発生器への入力として規定されるシード値から擬似乱数を生成するアルゴリズム処理手順である。かかる擬似乱数発生器は暗号システムでの大抵の乱数を生成するのには適していない。というのは乱数発生器の呼出し者は、入力として規定されるシード値を手許に持っていないか、または持たないことがよくあるからである。従って実際には、たいていの暗号システムでは動的にシードされる擬似乱数発生器を用いる便利な方法はない。代りに、これらの暗号システムでは初期にシードされる擬似乱数発生器または真の乱数を作成できる特殊ハードウェアを用いる。従って本発明の方法を実行するのが有利と考えられる所では、暗号システムは次の2つの乱数発生器を実行するのが必要であろう。

(1)は初期にシードされる擬似乱数発生器また真の乱数のハードウェア発生器であり、(2)は動的にシードされる擬似乱数発生器である。更に公用キーおよび私用キーが動的にシードされる擬似乱数発生器を利用して生成されることを許すキー生成アルゴリズムの設計を採用することが必要であろう。本発明のこれらの様子は以下に詳述する。

【0023】前に引用したUSP 4, 736, 423「RSA暗号変数記憶装置」は56ビットの機密値Xから50ビットの非機密値Yを計算する方法を述べており、400ビットモジュラスおよび400ビット指数を有する公用キーおよび私用キーを再生成するのにその後いつでも使用できる。これ以上大きな指数およびモジュラス長に対しては、yの長さはXが56ビット一定に留まっている間はほんの少し増加する。機密キー値Xはキー生成アルゴリズムへの入力として与えられ、公用キーおよび私用キーPU, PRの計算に加え、yの50ビット値をも計算する。値yがPU, PRを生成するのに始めにかかった時間に比べ、値yがXと共に公用キーおよび私用RSAキーPU, PRを非常に迅速に再生成できるという点で、値yは特別である。この手法は一方ではPU, PR(すなわち全指数とモジュラス)を記憶し、他方では必要になるたびにPU, PRを再生成するという両者間の妥協である。USP 4, 736, 423の手法はキーを再生成する短い計算ステップを必要とする代りに記憶しなければならないビット数を減らしている。本発明では、公用キーおよび私用キーをユーザが記憶しているパスフレーズから全部生成する。USP 4, 736, 423の方法が、入力パスフレーズをハッシュすることにより理論上は得られる56ビットの独立変数Xを利用しているのと対照に、数値Yは50ビットの従属変数である。すなわち公用キーおよび私用キーをポートするためには、ユーザは従属変数yをポートし、また暗号システムが公用および私用キーペアを再生成するように独立変数Xと共にそれを入力しなければならない。USP 4, 736, 423は本発明の利点の一部は有しているが、本発明ではパスフレーズ以外の追加情報とは独立に、キーをある装置から別の装置に移送することが可能である。従って、本発明ではUSP 4, 736, 423の方法では達成できないキーポートの形式が可能になる。

【0024】ここで開示する本発明の環境説明として、図3は通信ネットワーク10を示すネットワークブロック図であり、これにデータ処理装置20、データ処理装置20'、データ処理装置20''を含む多数のデータ処理装置が接続されている。また図3に示すように、各データ処理装置には暗号システムも含まれる。データ処理装置20は暗号システム22を含み、データ処理装置20'は暗号システム22'を含み、データ処理装置20''は暗号システム22''を含む。アプリケーションデ

ータの暗号化、解読、認証や暗号キーの生成、導入等に対する暗号サービスへのアクセスを要する複数のアプリケーションの処理手順を、各データ処理装置がサポートする。暗号サービスは各暗号システムの安全な暗号化機構により与えられる。データ処理装置が暗号化したデータおよびキーを送受信する手段をネットワークが提供する。各種のプロトコル、すなわち書式と手順規則が通信用データ処理装置間の相互使用性を確保するためその間の暗号量の交換を支配する。

【0025】図4はここで開示する発明の暗号システム22を示す。暗号システム22において、暗号化機構(CF)30は物理的インタフェースからの入力37を有している。暗号化機構アクセスプログラム(CFAP)34がインタフェース31により暗号化機構30に結合される。暗号キーデータセット(CKDS)32はインタフェース33により暗号化機構アクセスプログラム34に接続される。アプリケーションプログラム(APP)36はインタフェース35により暗号化機構アクセスプログラム34に接続される。

【0026】典型的な暗号サービス要求はインタフェース35にあるCFAP34への機能呼出しを通じAPP36により開始する。サービス要求にはキーとデータパラメータならびにインタフェース33のCKD32から暗号化したキーにCFAP34がアクセスするのに用いるキー識別子を含んでいる。CFAP34はインタフェース31のCF30に複数の暗号アクセス命令を発行することによりサービス要求を処理する。CF30にはCF30への暗号変数の直接入力のためのオプションの物理的インタフェース37を有することもできる。CF30によりCFAP34にリターンされる出力パラメータのセットを作成するために、CF31に呼出される各暗号アクセス命令にはCF30により処理される入力パラメータのセットを有する。交替で、CFAP34がAPP36に出力パラメータをリターンすることも出来る。CFAP34は以後の呼出し命令に出力パラメータおよび入力パラメータを使用することも可能である。もし出力パラメータが暗号化されたキーを含むならば、その時はCFAP34は、多くの場合これら暗号化されたキーをCKDS32に記憶することがある。

【0027】図5はここで開示する本発明の暗号化機構30を説明する。暗号化機構30は機密保護範囲140内で保全される。暗号化機構30には命令処理装置142を含み、これに実行コードとして具体化した暗号アルゴリズム144が結合している。暗号化機構環境記憶装置146は命令処理装置142に結合されている。図に示すように物理的インタフェースはライン37を通してCF環境記憶装置146に結合できる。命令処理装置142はインタフェース31により暗号化機構アクセスプログラム(CFAP)34に結合される。

【0028】命令処理装置142はインタフェース31

でCFAPアクセス命令により呼出された暗号マイクロ命令を実行する機能素子である。各アクセス命令に対し、インタフェース31は実行用特別マイクロ命令の選択に用いる命令ニーモニックまたは演算コードを先づ定義する。第2に入力パラメータのセットがCFAP34からCF30にパスされる。第3に出力パラメータのセットがCF30によりCFAP34にリターンされる。命令処理装置142は暗号マイクロ命令記憶装置144に記憶されたマイクロ命令として具象化された暗号処理ステップの命令の特定順序を実施することにより選択された命令を実行する。制御流れおよび暗号処理ステップのそれに続く出力は入力パラメータの値とCF環境記憶装置146の内容により決る。CF環境記憶装置146は例えば、キー、フラグ、カウンタ、CFコンフィギュレーションデータ等のCF30内に収集的に記憶される暗号変数のセットからなる。記憶装置146のCF環境変数はインタフェース31を通して初期化されるが、それは入力パラメータを読みとり、CF環境記憶装置146にロードする、あるCFマイクロ命令の実行による。代りに、初期化はオプションの物理的インタフェースを通して行うこともできるが、これは暗号変数を例えば付属キー入力装置を通す等、直接にCF環境記憶装置にロードすることができる。

【0029】暗号化機構機密保護範囲140の物理的実施例では次の物理的安全保護の特徴を備えている。物理的実施例は暗号化機構30へのアクセスを制限したインサイダアドバーサリによるプロービングに抵抗する。術語「制限した」というのは日、週でなく分、時間単位で測定される。アドバーサリ（敵）とは、高度の電子、機械設備を用いてアドバーサリの管理区域で発射される試験的攻撃と違い、制限された電子装置を用いてカスタマーの場所でのプロービング攻撃に限定される。物理的実施例はまた各種の電気機械式検知装置を用いて物理的プロービングまたはイントルージョンでの試みも検出する。またこの暗号化機構30の物理的実施例ではすべての内部に記憶された機密暗号変数のゼロ化を規定している。試みのプロービングまたはイントルージョンが検知されることがあると、自動的にこのゼロ化が行われる。物理的実施例はまた内部に記憶されている機密暗号変数のゼロ化に対する自動機能も備えている。前に引用したAbraham等の特許出願を参照すると、如何にしてこういった物理的機密保護の特徴を実行できるかの例が示されている。

【0030】キー生成プロセス：図6はこゝで開示する本発明の暗号化機構30に含まれる暗号アルゴリズム144を説明するブロック図である。図6を参照し、暗号アルゴリズム144には暗号化および解読演算を行う暗号アルゴリズム150、キー作成用にキー生成アルゴリズム（KGA）151および乱数作成用に乱数生成アルゴリズム152が含まれる。当面は乱数と擬似乱数とを

区別しないこととする。すなわち乱数生成アルゴリズム152は真の乱数発生器でも、または擬似乱数を作成するアルゴリズムであってもよい。乱数発生器と擬似乱数発生器については以下に論ずる。暗号アルゴリズム150はデータ暗号化アルゴリズム（米国標準規格X3.92-1981、データ暗号化アルゴリズム、米国規格協会、New York（1981年12月31日））等の対称アルゴリズムであってもよく、RSAアルゴリズムのような非対称、または公用キー、アルゴリズムであってもよい。公用キーアルゴリズムに対し、暗号化と解読との数学的演算間に差があってもなくてもよい。例えばRSAアルゴリズムでは暗号化も解読も共にべき乗演算モジュールとして実行される。暗号アルゴリズム150にはインタフェース153を通し命令処理装置142がアクセスし、このインタフェース153が命令処理装置142に暗号化および解読の基本演算を行わせている。インタフェース153は同時にキー、データ、その他の暗号変数が暗号アルゴリズム150と命令処理装置142との間を通るようにしている。同様の方法で、キー生成アルゴリズム151には命令処理装置142がインタフェース154を通してアクセスし、インタフェース154は命令処理装置142にキー作成を要求させる。インタフェース154は同時にキー、データ、その他の暗号変数が2つの各構成部品間にパスされるようにする。キー生成アルゴリズムはまた乱数生成アルゴリズムにインタフェース155を通してアクセスされる。これによりキー生成アルゴリズム151は、キー生成プロセスに必要な乱数生成アルゴリズム152からの乱数の要求、受理を行なう。乱数生成アルゴリズム152はまた命令処理装置142にインタフェース156を通してインタフェースをとり、命令処理装置142にキー作成以外の暗号化の目的に必要な乱数の作成を要求させる。

【0031】暗号アルゴリズム150がDEAのような対称または公用キー暗号アルゴリズムである場合は、キー生成アルゴリズム151によるキーの生成ステップは単純である。一般に、 n ビットキー（仮に $n=64$ とする）で生成するプロセスは次のステップから成る。64ビット乱数RNが乱数生成アルゴリズム152から要求される。ある場合には、RNは生成予定キーとして直接とられてもよい。しかし多くの暗号システムでは、キー生成には奇数パリティに対しキーの各バイトを調整するステップをも含んでいる。さらに他の場合では、キー値がある知覚された望ましくない性質を有さない、例えばキーが「実行時」あるいは「半実行時」DEAキーでないことを確かめるため、キー生成アルゴリズムがキー値をテストすることがある。「実行時」または「半実行時」DEAキーの規格に関しては、MeyerおよびMatyas共著、「暗号—コンピュータデータ保護の新次元」John Wiley & Sons社、New York、1982年を参照のこと。キーのパリティを

調節することは多くの暗号システムで共通の慣行であるが、大抵の場合、この追加テストは無視される。

【0032】暗号アルゴリズム150がRSAアルゴリズム等の対象または公用キー暗号アルゴリズムの場合、キー生成アルゴリズム151でもってキーを生成するステップがより多く含まれる。公用キー暗号システムでは、公用キーおよび私用キーペア(PU1, PR1), (PU2, PR2)等は特殊キー生成アルゴリズム(KGA)の助けをかりて作成される。KGAには、時にはKGAがその時キーの作成に用いる乱数の作成をKGAが作成または要求するプロセスの組合せを含んでいる。これら乱数はテストされ拒否されることがあり、他の乱数がある数学特性が満足されるまで要求されテストされることもある。さらに別の場合には、KGAがある乱数、またはある数学的特性あるいは複数の特性に対してテストされた後に受け付けた乱数値をとることがあり、この乱数値からその後1個以上の他の値を導出するであろう。一般に、KGAはキーの作成においてある単数および複数の乱数構成要素(すなわち乱数)を要求する。さもなければ、KGAが呼び出される度に同一の公用キーおよび私用キーペアが生成される恐れがある。この様なことは勿論許容されることでなく可能なキーペアのスペースから無作為に抽出され、または少く共無作為に抽出されているように思われ、従って敵がKGAが作成したキーペアを推測する手段がないことを保証するような公用キーおよび私用キーペア(PU1, PR1), (PU2, PR2)をKGAは作成しなければならない。上記のように、キーの作成において乱数を利用することに加え、KGAは数学的プロセスの使用を行い、このプロセスでは値は他の値(すなわち、構成的プロセスの使用)から計算または導出され、試行錯誤のプロセスを用いて値を計算する(すなわち、所要の値が見つかる迄試行値をテストし拒否する)。好ましい実施例ではキー生成アルゴリズム中で直接シード値を用いるよりも寧ろ擬似乱数発生器を初期化するのにシード値を用いている。その理由はシード値が必然的に、キー生成アルゴリズムがシードにおけるより多くのランダムビットを必要とするであろうという非ゼロ確率が存在していることを意味する特定有限長であるのに対し、擬似乱数発生器はキー生成アルゴリズムが必要とするだけ、任意長の擬似乱数を生成することが可能だからである。もしキー生成アルゴリズムがシードよりも多くのランダムビットを要することが起れば、シード値の直接再使用は許容されないことになるであろう。その理由は、キー生成アルゴリズムはすべてのテスト基準を満足する出力への値を見出せないことがあるので、計算を完了できないことがあるからである。動的にシードされる擬似乱数生成アルゴリズムを使用すると擬似ビットの任意数の使用可能性を保証することにより、この潜在的無限くり返しは避けられる。

【0033】図7は暗号アルゴリズム150がRSAアルゴリズムである時のキー生成アルゴリズム151を説明する流れ図である。キー生成アルゴリズム151は公用キーおよび私用キーペア $PU = (e, n)$ および $PR = (d, n)$ を作成する。ここで e, d は公用および私用指数(e, d は n より小の正の整数)と呼ばれ、 n は公用モジュラスである。従って2個組 (d, n) において、私用指数 d のみが機密保護を必要とする。図7を参照し、ステップ161で p の試行値が生成される。ステップ162で、 p の値が素数性に対してテストされる。素数性テストの方法を以下に述べる。 p が素数ならば、制御はステップ163に進む。そうでなければ制御はステップ161に戻る(すなわち新 p が生成される)。ステップ163で p が「強」素数であるかどうかを調べるテストが行われる。「強」素数とは、選定した p が素数 p, q にモジュラス n を因数分解することにより暗号アルゴリズムを「ブレイク」するための数学的解析を許可しないことを保証する追加基準集合を満足する素数 p を表わす本手法での術語である。キー生成および p, q が暗号攻撃を妨げるのに充分強であることを保証するために p, q について実施される追加テストの論議に対しては、Rivest, R. L., Shamir, A., Adleman, L. 「デジタルシグニチャおよび公用キー機密システムを得る方法」を参照のこと。ステップ163で p について実施される追加テストには、 $p-1$ が大素数因数 p' を有することおよび $p'-1$ が大素数因数 p'' を有することのテストが含まれる。RSAキー生成について述べている文献で示唆されるその他のテストとして $p+1$ が大素数因数を有することをテストするものもある。 p が「強」素数ならば制御はステップ164に進み、その他の時は制御はステップ161に戻る。(すなわち新しい p が生成される)。ステップ164で q の試行値が生成される。ステップ165では p の値が素数性についてテストされる。 p が素数なら、制御はステップ166に進み、その他の時はステップ164に戻る(すなわち新しい q が生成される)。ステップ166で q が「強」素数かどうかテストされる。ステップ166で q に実施される追加テストには $q-1$ が大素数因数 q' を有することおよび $q'-1$ が大素数因数 q'' を有することのテストを含む。RSAキー生成を論ずる文献が示唆する別のテストは $q+1$ が大素数因数を有することをテストすることである。もし q が「強」素数ならば、制御はステップ167に進み、その他の時は制御はステップ164に戻る。(すなわち新しい q が生成される)。ステップ167で公用モジュラス n は p と q の乗算積として形成される。ステップ168で、値 r は $(p-1)$ と $(q-1)$ の乗算積として構成される。ステップ169で、キー生成アルゴリズムにより、公用指数 e が入力として与えられているかどうか決定される。もし入力として与えられるならば、その時には制御はステ

ップ172に進み、与えられた値 e がステップ171でテストされた条件を満たすと仮定される。別の実施例としては、制御がステップ171にフローすることができ、与えられた値 e をキー生成アルゴリズム151によりチェックすることもできる。もし入力として与えられなければ、制御はステップ170に進み、ステップ170で e の試行値を生成する。ステップ171で e が r に対し相対的に素であることを確認するためのテストを行なう。これは容易に実行され、 e と r の最大公約数(GCD)が1であること、すなわち e と r が1以外の共通因数を有しないことをチェックする。 e と r が互いに相対的に素であれば、その時は制御はステップ172に進み、その他の時は制御はステップ170に戻る。(すなわち新しい e が生成される。)ステップ172で、値 d は e と d との積が1モジュロ r と合同であるように計算される。ステップ173で $PU = (e, n)$ と $PR = (d, n)$ の計算値が出力としてリターンする。

【0034】素数性に対し多数をテストする適切な手法の1つに、R. Solovay, V. Strassen が「素数性に関する高速モンテカルロテスト」SIAM Journal on Computing, 1977年3月, ページ84, 85で述べた有効な「蓋然論(probabilistic)」アルゴリズムの使用がある。ここでは乱数「 a 」を一様分布(1, 2, ..., $X-1$)からとり、「 a 」の最大公約数および X が1であるかどうか、すなわち $GCD(a, X) = 1$ をチェックし、また $J(a, X)$ で表わす「 a 」と X のヤコビの記号が Q モジュロ X に合同かどうか(ただし Q は「 a 」の $(X-1)/2$ べき乗に等しい)をテストする。ここで整数(a_1, a_2 , 等)の集合(但し集合中の各「 a 」は X より小さい)を用いて X を素数性に関してテストする。図7に示すように、RSAキーを生成する場合には値 X を値 p, q に置き換えることに注意する必要がある。このテストでは、セット中の各「 a 」の値に対し、上記の両条件が保持されることが必要である。従って集合中に両条件が保持されない「 a 」があれば、 X は複素数であることが分かる。その他の時は X は素数として受容される。この手順は選択した数が素数であることを保証するのではなく、素数性のテストに失敗しなかったことのみを保証している。集合中の整数 a (a_1, a_2 等)の数が大きい程、選択した数が素数である確率が大い。たゞし勿論集合中の各整数「 a 」に対し両条件が満足されていることが仮定されている。2整数の最大公約数、2整数の最小公倍数、2整数のヤコビの記号の計算法は技術上周知である。

【0035】適切な暗号保護を達成するRSAアルゴリズムに対し、モジュラス n がほぼ512ビットと1024ビット間の数であることが必要ことは当業者によく知っている。前記のキー生成アルゴリズムでは、公用キー指数 e はキー生成アルゴリズムに規定することも、キ

ー生成アルゴリズムにより生成することも可能である。 e をキー生成アルゴリズムに規定する利点は小さな値(例えば $e=3$)を規定できることである。公用キーで暗号化する時はこれにより性能が向上する。私用指数 d は従属変数であり、導出されなければならない。従って実用上は、 d はモジュラスと同一サイズになる。この場合モジュラスが512ビットなら、選択した指数 e のビット数により、公用キー PU は514ビット~1024ビットであり、他方私用キー PR は1024ビットである。64ビットまたは128ビットのDEAキーと比べると、RSAキーはかなり大きい。当業者には公用キーアルゴリズムが可成り計算的に強力な手順であることも認められる。単一の公用キーおよび私用キーペアを生成するのに必要な時間で、数千、恐らく数百万ものDEAキーを生成できる。固定ブロックサイズのDEAと違って、RSAアルゴリズムは特定のブロックサイズを要しない。そのために選択したモジュラス長により、RSAキー生成が比較的短かったりまたは比較的長いプロセスであったりすることができる。キー生成アルゴリズム151が希望サイズ(すなわち規定ビット数)の公用キーおよび私用キーを生成するためには、生成された p と q が共に掛け合わせると希望のサイズ、あるいはビット長のモジュラス n を生ずるようにステップ161と164とを設計する。 p, q に関する追加テストを図7の流れ図に追加でき、これによりISO Draft Internal Standard 9796「メッセージ回復を与えるデジタル署名計画」のような暗号規格中で規定されることのある仕様に従って、キー生成を適合させ得ることに当業者は理解するであろう。また図7に述べたRSAキー生成アルゴリズムは、 p と q の作成が単に試行錯誤法ではなく、試行錯誤とその値を構成する方法とを組合せるプロセスで行うならば、より効率が上るということを当業者は認めるであろう。 p の生成、 $p-1$ が大素数 p' を有することのテスト、 $p'-1$ が大素数 p'' を有することのテストの代りに、大素数 p'' を生成することから開始することも出来る。この場合、少数を p'' に乘じ、1を加え、次にプライマリティのテストをすることにより p'' から素数 p' を見つける。この結果得られた p' が素数でなければ、 p'' に別の少数を乗ずる以外は同じプロセスを繰り返す。同じ手法で p' から p も見出すことができる。同様に、同じ手法を使って q'' から q を見出すことができる。

【0036】RSAキー生成には多くの変形がありうることを当業者は認めるであろう。しかしどんな場合にも、キー生成プロセスでは乱数が必要であり、この乱数は乱数発生器または擬似乱数発生器を用いて作成することが出来る。図7に戻ると、ステップ161, 164では p, q の試行値が無作為に生成される。一度生成されると最も重要性の少ない(低位または右端)ビットをB「1」に等しく設定することができ、生成値が必ず整奇

数であることが確実となる。値2を除きすべての素数は奇数であるから、これにより処理が速くなる。上述のように p と q を p'' と q'' とから生成する場合は、 p'' と q'' の試行値を無作為に生成する。公用指数 e がキー生成アルゴリズム151に入力として与えられていない時には、 e の試行値を無作為に生成する。このようにして、すべての場合に、RSAキー生成には乱数の作成と使用の必要なことが分る。

【0037】乱数および擬似乱数：大抵の暗号システムでは乱数を作成、使用する手段が必要である。例えば、DEAによる暗号化の暗号ブロック連鎖モードを使用する時など、乱数を初期化ベクトルまたは初期連鎖値として使用する。例えば、DEAによる暗号化の暗号フィードバックモードを使用する時などは、乱数を「シード」値として使用する。多くの暗号ベース識別および認証プロトコルでは乱数をその場限りに使用する。乱数作成能力がないと、大抵の暗号システムは著しく制約を受けるかまたは使いものにならないであろう。

【0038】図8および図9に暗号システムで乱数を生成するのによく用いられる2方法を示す。図8は「真」乱数発生器180のブロック図である。「真」乱数発生器180にはハードウェア回路181を含み、乱数を作成する能力がある。かかるハードウェア発生器で乱数を作成する手段はよく知られており従来技術で実行できる（前記USP4,905,176、R. Schulz「乱数発生器回路」1990年2月27日発行を参照）。乱数の要求はインタフェース182を通して入力される。生成された乱数（RN1、RN2等）はインタフェース183を通し出力される。実際には生成された乱数の長さはアルゴリズムの固定定数例えば64ビットである。「真」乱数発生器はその出力値が予想不能であるという性質を有する。すなわち乱数発生器の出力を予測するようなアルゴリズムを構成する筈はない。「真」乱数発生器は初期化にシード値を必要とせず、従って発生器の出力を繰り返させる方法は存在しない。この性質が「真」乱数発生器を暗号システムでの実行を非常に望ましいものにしている。しかし「真」乱数発生器のコストは擬似乱数発生器に比べて比較的高いため、大抵の商用暗号システムは擬似乱数発生器を使用している。

【0039】図9は初期にシードされる擬似乱数発生器190のブロック図である。初期にシードされる擬似乱数発生器190にはアルゴリズム191および乱数生成にアルゴリズム191が使用するシード値記憶のためのシード記憶装置194を有する。（擬似乱数発生器により作成された乱数は一見無作為に見えるだけであることに注意を要する。より正確には、擬似乱数発生器により作成される出力は擬似乱数と呼ぶべきである。しかし便宜上これらも乱数と呼ぶことにする）。初期シード値はインタフェース195を通し指定される。初期シード値自体は暗号命令の1つを通し暗号機構にインタフェース

するユーティリティプログラムを通し暗号システムに入力されるか、または入力されたパスワードあるいは物理的なキー操作スイッチを用いて許可されたインストラクション要員のみが操作できる特殊前面パネルインタフェースを通し入力される。キー生成に擬似乱数発生器を使用する場合は、初期およびその後すべてのシード値は機密にしておかなければならない。そうでなければ、擬似乱数発生アルゴリズムは公用領域にあると考えられるから、生成された乱数の機密度はシード値を秘密にしておくことに依存している。乱数を生成する時には、シード値はアルゴリズム191の性質にもよるが、アルゴリズム191により動的に更新されることがある。アルゴリズム191にはまた、乱数作成中自動的に更新されるカウンタ数またはシーケンス数の記憶装置のような、別個の記憶装置を有するものがある。この場合には、シード値は一定のまゝでカウンタ数またはシーケンス数のみが更新される。カウンタ数またはシーケンス数を用いるケースでは、シード記憶装置194にシード値がインタフェース195を通して初期化される時に初期値がアルゴリズム191によりセットされる。乱数の要求はインタフェース192を通し入力される。生成された乱数（RN1、RN2等）はインタフェース193を通し出力される。実際には生成された乱数の長さはある固定値、例えば64ビットである。擬似乱数発生器はその出力が完全に予想可能であるという性質を有す。擬似乱数発生器の出力は一見無作為に見える数値の列（RN1、RN2等）である。アルゴリズムがいわば「メモリ」を有している理由のみで、RN2はRN1とは違っている。すなわち、アルゴリズムは連続的に自身を更新しており、アルゴリズムが呼び出される度に違った「出発」点から始まる。しかし、もし同じアルゴリズム191の各場合が同じシード値で初期化されたとしたら、各アルゴリズム191により作成される乱数は完全に同一となる。初期シード値自体を無作為プロセスを通して選択すべきであるということが良い暗号実施法である。こうすると別々の暗号装置で各々初期にシードされる擬似乱数発生器190は異なる乱数を作成する。

【0040】図10は動的にシードされる擬似乱数発生器200のブロック図である。動的にシードされる擬似乱数発生器200は乱数発生用にアルゴリズム201を有する。乱数の要求はインタフェース202を通し入力される。生成された乱数（RN1、RN2等）はインタフェース203を通し出力される。インタフェース203で生成された乱数（RNと名付ける）の長さはインタフェース202における長さパラメタにより規定される値に等しい。アルゴリズム201には内部に記憶されたシード値を有しない。その代り要求されるシード値はインタフェース202においてアルゴリズム201に指定される。このシード値は呼出し者に見えなければならないが、それは同一シードを入力すれば同一出力が生ずる

ことを保証しながら他の呼出し者による要求のインタリーブを行なえるからである。便宜上、長さ値が生成される乱数長を決める所では、アルゴリズム201では長さパラメタをインタフェース202で指定してよい。実際上は、シードの長さは大抵はアルゴリズム201が予め設定した固定数である。動的にシードされる擬似乱数発生器200の演算を説明するため次のことを仮定する。(1)パラメタ「長」はビットで指定され、(2)パラメタ「シード」のビットでの長さは128であり、Lは望ましい乱数(RNと称する)のビットでの長さである。その場合パラメタ「長」で指定される値は128+L、すなわち次期シードの長さプラス望ましい乱数の長さで計算される。

【0041】別の実施例では、次期シードの作成を自動的に行うと、従ってパラメタ「長」は望ましい乱数RNの長さを指定することになる。その場合は、インタフェース203では2つの出力、次のシードとRNがある。いずれの実施例も作動する。最初の場合では、動的にシードされる擬似乱数発生器200は次期シードを作成する方法については意識しない。次期シード値の作成、管理は呼出し者の制御下にある。第2の場合では、動的にシードされる擬似乱数発生器200は呼出し者に次期シード値を計算して戻す責任がある。

【0042】さらに別の代替実施例では、初期にシードされる擬似乱数発生器のアルゴリズムと動的にシードされる擬似乱数発生器のアルゴリズムとが同じアルゴリズムであり、アルゴリズムには同一の回路および/またはルーチンを用いることができる。初期にシードされる発生器は普通のユーザではアクセスできないシステム記憶装置を用いてシステムシード値を有し、これは初期にシードされたアルゴリズムが呼出されると必要に応じて自動的に更新される。また動的にシードされる発生器は呼出し者にそのシード値をパス(および維持)するように要求する。上記方法に対し小修正や変化を加えた多くの実施例が可能であり、この相異点は本発明に何等影響しないことを関係者は認めるであろう。

【0043】本発明では、公用キーおよび私用キーペア(PU, PR)はユーザによる入力として機密パスフレーズから生成されており、その実行のためにはキー生成アルゴリズムが同じ順序の乱数を再生成するし、従って同じパスフレーズがキー生成アルゴリズムに指定される度に同じキーペア(PU, PR)を再生成することが出来る。これが極めて重要である。これと対照的に、暗号システムで乱数を要求する他の暗号アプリケーションは全て、同じ順序の乱数を再生成する必要を有しない。実際には、かゝる能力が暗号システムに存在するとキーが偶然再生成されるような好ましくない状態に通ずる可能性があると言われることもある。

【0044】図8、および図9に示す方法によりキー生成アルゴリズムが要求する乱数を作成する場合には、再生

成従ってパスフレーズから公用キーおよび私用キーペア(PU, PR)を生成することは不可能である。図8の「真」乱数発生器180は、キーペア(PU, PR)を満足に再生成するために必要となる同一順序の乱数を再生成させる方法がないので、使用することが出来ない。同様に、図9の初期にシードされる擬似乱数発生器190も、同一順序の乱数を再生成せしめる方法を有しないので使用出来ない。実際には、暗号システムに電源が入りラインにつながった時、または時には装置の電源が切れていた期間の後で一度だけかゝる擬似乱数発生器が通常初期化される。その後は単に乱数を要求するだけでよい。すなわち動的にシード値を再指定する用意はない。多くの場合呼出し者は手許にシード値を有さない、擬似乱数発生器の各呼出し者に彼自身の「シード」値の入力を要求するよりも、むしろ一度だけ擬似乱数発生器に「シード」する業務を行うのが最も良い。事実多くのシステムユーザが使用すると考えられるこの形式の擬似乱数発生器に、通常のユーザがシード値を指定できないということは機密保持の観点から重要である。

【0045】以上の説明から図10に図示する動的にシードされる擬似乱数発生器は、本発明の要求を満足できるが、大抵の暗号システムにおいては乱数作成の一般要求を満たさないことは明らかである。同様に前記の説明から、図8に示す「真」乱数発生器および図9に示す初期にシードされる擬似乱数発生器は大抵の暗号システムにおける乱数作成の一般要求を満足できるが、キー生成アルゴリズムがパスフレーズからキーを再生成しなければならない時の乱数作成の要求を満足しない。従って、本発明の好ましい実施例においては、図11に示すように乱数生成用に2手段が必要とされる。図11を参照すると、図6で前に図示した暗号化機構の暗号アルゴリズム144構成品は動的にシードされる擬似乱数発生器200およびキー生成アルゴリズム151と動的にシードされる擬似乱数発生器200間のインタフェース204を含むように拡張されており、乱数要求によりリターンすべき乱数を生成せしめる。図11の動的にシードされる擬似乱数発生器200は既に述べた図10の動的にシードされる擬似乱数発生器200と同一に作動すると仮定されている。すなわち、乱数要求には長さとしードの指定を含む。出力は乱数である。キー生成アルゴリズム151はシード値を管理すると仮定される。例えば第1シードはこれから述べる方法を用いてパスフレーズから計算する。キー生成アルゴリズム151が長さLの乱数を要求する時はいつもL+128の「長さ」パラメタを指定する。すなわち次期シードを自動的に要求し、キー生成アルゴリズム151にアクセスできる次期シード格納域に保管する(例えばキー生成アルゴリズム151内に)。図11のキー生成アルゴリズムが図7のRSAキー生成アルゴリズムそのものである場合には、図7のステップ161、164、170が図11のインタフェー

ス204での動的にシードされる擬似乱数発生器200に向けられる乱数の要求になるであろう。従って図7のステップ161, 164または170が繰返される度に、新乱数が得られる。満足な値を見出すまでにどれだけの試行を必要とするかを予め知る方法はなく、プロセスは試行錯誤であるから、乱数の順序を予め計算出来ず必要の都度試行を行う。

【0046】図12は本発明の要求を満足する動的にシードされる擬似乱数発生器の例である。アルゴリズムは128ビットを要し、これを64ビットキーKと64ビット初期連鎖値ICVとに分割する。シードの左側64ビットがKになり、シードの右側64ビットがICVになる。mを発生する無作為ビットの数とすると、64nにmより大の最小値を表わさせる。ここでnはmビットの擬似ランダムシーケンスを作成するのに充分の長さを有する生成すべき暗号文の64ビットブロックの数を表わす。暗号文を生成するのに、2進ゼロのn64ビットブロックでスタートし、DEA暗号化の暗号ブロック連鎖モードを用いてDEAアルゴリズムで暗号化する。キーと初期連鎖値は上記のKとICVそのものである。長さmの出力乱数RNは結果の暗号文における左側（最も重要な）mビットそのものである。

【0047】パスフレーズを使用するキー生成：図13は暗号システムを図示しており、暗号化機構（CF）30、暗号キーデータセット（CKDS）32、暗号化機構アクセスプログラム（CFAP）34およびアプリケーションプログラム（APPL）36を有する。ここで図13を参照すると公用キーおよび私用キーペア（PU, PR）を生成するステップをトレースできる。40においてアプリケーションプログラムA（APPL A）42がユーザにより呼び出される。APPL Aは

（1）アプリケーションが処理とつながる以前にユーザが自分のキーを生成または再生成することを要求するアプリケーションであるか、または（2）ユーザがそれらのキーを生成または再生成することを許容するユーティリティであることを仮定している。APPL Aは、ユーザが41で入力するパスフレーズ（PPと称する）をユーザに催促する。応答して、APPL Aは43でキー生成機能47をコールする。43はCFAP34にあり、モードパラメータPPおよび制御情報をパスする。制御情報は制御ベクトルまたは制御ベクトルをつくるのに用いられる情報であってもよい。モードパラメータは生成キーがパスフレーズベース（モード＝「PP」）で生成されるか、されないか（モード＝「非PP」）いずれをキー生成機能に指示する。従ってPPパラメータは選択パラメータである。制御情報はキータイプ（すなわち生成すべき公用キーおよび私用キーのタイプ）およびキー管理でのキーの使用法を示す取扱い制御情報である。応答して、キー生成機能47は（1）入力パラメータをパースし、（2）もしモード＝「PP」なら入力パ

スフレーズPPから128ビットハッシュ値CWを計算し、入力制御情報を処理し、GRVPR命令を指定される制御データパラメータを作り、GPUPR命令52を呼び出して50で暗号化機構30の命令処理装置142で実行する。50はモードパラメータおよびもしモード＝「PP」ならオプションコードワードCW、および制御データをパスする。制御データには生成すべき公用キーPUと関係するキー関連情報を指定するPU制御ベクトルおよび生成すべき私用キーPRに関連するキー関連情報を指定するPR制御ベクトルを含む。各制御ベクトルには暗号システム内のキーを識別するキー名を含んでいる。各制御ベクトルは同時にラベルまたはCFにより初期化されるべきCKDSラベルの予約スペースを含み、暗号キーデータセット（CKDS）32からのキートークンの記憶、検索に用いることができる。応答して、GPUR命令52は、図14に、より詳細な記述があるように、入力としてモードパラメータ、またもしモード＝「PP」ならコードワードCWをパスして、キー生成アルゴリズムKGAを呼び出す。応答して、KGAは図14に詳細記述があるように公用キーおよび私用キーPU, PRを生成し、GPUPR命令52にリターンする。応答して、GPUPR命令52は生成されたPUを含むPUキートークンおよび生成されたPRを含むPRキートークンをつくる。PUキートークンおよびPRキートークンは図15に説明されており、以下詳しく述べる。GPUPR命令は以下詳細説明するように、同時に50で入力としパスされるモードおよび制御データについて一貫性チェックを行う。一貫性チェックにより、キータイプと各キートークンの制御ベクトル部分の取扱い情報とがモードと一致していること、すなわちキーがパスフレーズから生成されたか否かが確められる。PU, PRキートークンは次にキー生成機能47に51でリターンされる。応答して、キー生成機能47は必要ならPU, PRキートークンを更新する。例えばCKDSラベルの記憶装置に対するトークンの予約フィールドがこの時点で埋められる。次にキー生成機能47はキー記憶装置マネージャ46にCKDS32の1個または2個のキートークンを記憶させ、44でAPPL Aにキー名またはラベルのみをリターンさせるか、または44でAPPL Aに1個または2個のキートークンをリターンする。ここで意図はAPPL 42にキートークンを管理、制御させる（もしそう望むなら）か、暗号システムにキートークンを管理、制御させることである。どちらの進め方にも利点があり、キートークンがCKDS32に記憶されるにしても、あるいはAPPL 42にリターンされるにせよ、キートークンの取扱いは43でのキー生成機能47へのAPPL A42により指定される入力パラメータの制御下にあるように暗号システムを設計することが可能である。応答して、APPL Aは必要に応じキートークンを記憶するか、またはCFAPで

実行する他の暗号機能への入力として、PU、PRキートークンが後で再指定できるキー名またはラベルを記憶する。ここでAPPL Aはユーザに、要求された公用キーおよび私用キーが入力パスフレーズから生成されたということを指示する。APPL Aは処理が完了する時迄必要に応じ処理を続ける。生成したキートークンの1個以上がCKDS 3 2に記憶されたと仮定すると、APPL Aは4 5でキーページ機能4 8をコールする。4 5はCFAP 3 4にあり、ページされるべき各キートークンのキー名またはラベルをパスする。応答して、キーページ機能4 8はキー記憶装置マネージャ4 6にCKDS 3 2から各キートークンを抹消させる。もしAPPL Aがキートークンを管理しているなら、キーページ機能4 8をコールする代わりに、APPL Aがキートークンをページする。図1 3には示されていないが、各呼出しエンティティには適当なリターンコードおよび条件コードを利用できると仮定されており、従って要求された処理が正常に完了したこと、あるいは追加の処置を要するエラーが発生したかどうかの指示を呼出しエンティティは有している。キー生成機能4 7およびGPUPR命令5 2は次の2タイプのキー生成を操作するように設計されていることを当業者なら認識できる。(1) PU、PRがパスフレーズから生成される場合(モード=「PP」)、(2) PU、PRがパスフレーズから生成されない場合(モード=「非PP」)。すなわち、キー生成機能およびGPUR命令の設計は本発明の好ましい実施例であると考えていることをベースにしている。その理由は、いずれのモードとも両方の種類のキー生成を行うことは出来ず、また各モードは今論じた通りキー管理においてそれぞれ独自の異なる利点を有するからである。

【0048】公用キーおよび私用キーペア(PU、PR)が生成される時、このキーがパスフレーズから生成されたものであるか否かを識別することが重要である。基本的にはパスフレーズから生成されたキーはユーザに知れるキーである。直接には知れなくとも、このキーはユーザが計算でき、従って厳密な意味ではユーザに知られる。これはPU、PRの計算に用いられるアルゴリズムは公用領域にあると推定されるからである。すなわち機密が保たれる根拠がない。唯一の機密要素はパスフレーズその物である。従って、パスフレーズを知る人はキーを知る(または計算する)ことができる。しかし公用キーおよび私用キーペア(PU、PR)がパスフレーズから生成されない時、すなわちキー生成プロセスに含まれる無作為要素または無作為値が真の乱数発生器(図8)か、初期にシードされる擬似乱数発生器(図9)のいずれかを用いて暗号機構で生成される時は、キー生成アルゴリズムにより生成されるキーはすべての実用目的に対してはユーザには知られないかまたは知ることができないものである。(多くの場合、キーはマスタキーの

下で暗号化されており、生成されるキーはマスタキーと同程度の機密度を有す。マスタキーを知る人は誰でも生成されるPUとPRも知ることになるが、PUは公用キーであるから懸念する要はない。)「スマート」キー管理設計では、両タイプの生成キーを利用することができる。パスフレーズから生成されない私用キーPRは、理論上は暗号システム自体によってのみ知ることが出来る。従って適正に実行するなら、完全性のシステムレベルあるいは機密性のシステムレベルの実行にこういったキーを用いることができる。これはPRがユーザに知られるならば達成されないものである。反面ユーザに知られるPRにより、よく利用される多くの機能がある。例えば、暗号システムにそのユーザを認証する、またはそのユーザを他のユーザに認証する、または情報をそのユーザから来ていると認証する(例えば、ユーザが計算して彼のメッセージにデジタル署名を添付する場合)のにPRは使用される。キー管理設計は次の方法でこの差を利用することがある。GPUPR命令5 2の処理の一部として、PU、PRキートークンを作るステップがある。

【0049】図1 5にPUキートークンおよびPRキートークンの書式を示す。PUキーは公用キーであるから、PUキートークンはクリアまたは暗号化されたフォームeKM. H1 (PU)でPUを記憶することがある。ここでKM. H1はCF 3 0のCF環境記憶装置1 4 6内に記憶されている機密マスタキーKMと暗号変数H1との排他的論理和積であり、H1は中間ハッシュ値1を作成するのにC1をハッシュし、またH1を作成するのにハッシュ1に数ビットをフィックスすることによりPUに対し制御ベクトルから作成される。eKM. H1 (PU)の正確な規格は前記のS. M. Matyas等による同時係属特許出願「制御ベクトルを用いる公用キー暗号システムキー管理」に述べられている。PRキーは私用キーであるから、PRキートークンは暗号化したフォームeKM. H2 (PR)でのみPRを記憶する。eKM. H2 (PR)の正確な規格は前記のS. M. Matyas等による同時係属特許出願「制御ベクトルを用いる公用キー暗号システムのキー管理」に述べられている。PUとPRを暗号化する暗号化変数H1とH2は異なっている。H1は公用キーPUに関連する制御ベクトルC1より導出し、H2は私用キーPRに関連する制御ベクトルC2より導出する。PU、PRキートークンは、それぞれキー名またはCKDSラベル、使用法制御情報等のキー関連データである制御ベクトルC1、C2も含む。PU、PRキートークンにはまたフォームeKM. H1' (KAR)、eKM. H2' (KAR)の確証を含んでいる。たゞしCKARはキー確証レコードであり、H1'、H2'はH1、H2に係わる暗号化変数である。KARはクリアまたは暗号化キーすなわちPU、eKM. C (PU)またはeKM. C (P

R)の暗号機能である。eKM、H1' (KAR)およびeKM、H2' (KAR)の正確な規格は前記のS. M. Matyas等による同時係属特許出願「制御ベクトルを用いる公用キー暗号システムのキー管理」に述べられている。PU、PRキートンにはキートン中に他のフィールドの記憶位置と長さを識別する情報を有するヘッダ部分も含んでいる。これによりそのフィールドを可変長にすることができる。

【0050】図16にはPU、PRキートンの制御ベクトル部分の追加規格を示す。図16を参照すると、制御ベクトルにはCVタイプと名付ける制御ベクトルタイプフィールドを含んでおり、キーが公用キーか私用キーか、さらにそのキーはユーザキーか、キー管理キーか、証明キーか、あるいは認証キーを示す。4つのキータイプ(ユーザ、キー管理、証明、認証)の正確な識別は本発明では重要ではない。しかし、異なるキータイプはキー管理設計において異なる目的と用途を有することを理解するのは重要である。例えば、タイプ=「ユーザ」と制限して、公用ユーザキーがデジタル署名を生成するためのみに用いられることができる。他方タイプ=「キー管理」はより広範であり、私用キー管理キーを暗号化の目的に、またある暗号装置から他の暗号装置にDEAキーを分散する目的に使用することも、また公用キー管理キーにデジタル署名を生成させることも可能である。例えば、公用キー、私用キーペアはキーを暗号化するDEAキーを分散するために2つの暗号システム間で用いることができる。その後は、キーを暗号化するキーは他をDEAキーを2つの夫々の暗号システム、例えばデータキー間に分散するのに用いられる。この場合は、一般にはこの目的に公用ユーザキー、私用ユーザキーを用いようとはしないであろう。その理由は、この場合は、自分の私用ユーザキーを知っているか、または理論的に知りうるユーザ自身はキーを暗号化する暗号化されたキーをインタセプトし(すなわち、PUで暗号化されたキーを暗号化するキー)、またそれを自分の私用キーPRで解読することができるからである。このようにして、ユーザはキーを暗号化するクリアキーの値を見出すことが可能であり、たいいていの暗号システムではキー分配プロトコルの所期の機密保護に打ち勝つことになる。従って、PU、PRキートンをGPUPR命令52が作る時点において、生成されたキーのキータイプおよび使用法が意図されたキー管理設計に合致することを確認するため50での入力として指定されたモードに対し、図14の50での入力として指定されたPU、PR制御ベクトル(または等価的には図13の50での制御データ)に関する一貫性チェックをGPUPR命令が実行しなければならないことは本発明の一部である。例えばCFAPがモード=「PP」を指定し、制御データがタイプ=「キー管理」を指示するならば、その時はGPUPR命令52はこの不一致を検出し、キータイプに

対する不一致指示により処理を停止したというCFAPへの指示でもって演算を打ち切らなければならない。他方では、もしCFAPがモード=「PP」を指定し、制御データがタイプ=「ユーザ」を指示するならば、その時はGPUPR命令52はキータイプの不一致により演算を打ち切ってはならない。ここでは述べないが、追加の一貫性チェックがGPUPR命令に演算を打ち切らせることがあることに注意を要する。キートンに生成されたキーがキータイプおよび使用法を指定する制御情報に連結されることは重要であるから、本発明の好ましい実施例では図15のPUキートンは、暗号化された書式eKM、H1(PU)でPUを記憶しなければならない。前記のように、H1をキートンの制御ベクトルに従属させることにより、これが達成される。H1を制御ベクトルに従属させる正確な方法はここでは重要でないが、前記のS. M. Matyas等による同時係属特許出願「制御ベクトルを用いる公用キー暗号システムのキー管理」に詳細が述べられている。前述から、本発明はユーザ供給のパスフレーズから公用キーおよび私用キーペアを生成する手段を提供することは理解されるであろう。しかし大抵の暗号システムでは、上記のようにユーザが私用キーPRの値を予測したり、決定する能力を有さないような方法で、公用キーおよび私用キーを暗号システム内で生成する時には、より機密保護された設計が可能である。従って本発明では、キーペアがパスフレーズから導出されたか、またはキーペアがパスフレーズからは導出されていないかによって、生成されるキーのタイプの双方の使用法を制御する手段も提供するものである。従来技術(USP4,941,176、4,918,728、4,924,514、4,924,515、5,007,089)では制御ベクトルを通してキータイプおよびキー使用法を制御する手段が述べられている。しかし、この従来技術は、キーが如何にして生成されるかに従ってキーのタイプと使用法を制限する方法は述べていない。対照的に、本発明は公用キーおよび私用キーがパスフレーズから生成されるキーと、パスフレーズから生成されていないキーとを区別し、指定されるキータイプが許可すべきか、または許可すべきではないかをキー生成命令(すなわちGPUPR命令)内で決定する手段として、この区分がキー管理に重要であることを示した。このようにして本発明は生成プロセスを適当に制御する手段を提供し、そのため生成されるキーは、キーのタイプおよびそれが暗号システム内で如何に処理されるかを指定する制御ベクトル情報に、適当に暗号的に連結されることになる。生成されるキーを制御するこういった手段がなければ、パスフレーズおよびパスフレーズから生成されるキーの利点は暗号システムの全体機密保護を弱めるように思われ、パスフレーズから導出するキーの利点は利点ではなく欠点となるように思われることになろう。従って、本発明は単にパスフレーズ

からキーを生成する手段を提供するのみではなく、キー管理内で生成されたキーを制御する本質的な手段をも提供するものである。

【0051】図14は、GPUPR命令52を呼び出す結果としてCF30内で実行される演算の説明である。図14のGPUPR命令52は、図13のGPUPR命令52とは、図14がキー生成アルゴリズム152および動的にシードされる擬似乱数発生器200を呼び出す追加のステップがあるという点以外は全く同一である。図14を参照すると、50での入力にはモード、オプション命令語（CWと呼ぶ）、PU制御ベクトル、PR制御ベクトルよりなる。図13では、PU制御ベクトルおよびPR制御ベクトルは単に制御ベクトルと呼ばれている。呼び出されたことに応答して、GPUPR命令52は53でキー生成アルゴリズムKGA152を呼び出し、モードパラメータおよびオプションCWをパスする。応答して、KGA152はキー生成を実行するステップを遂行する。例えば、CF30内で行われる暗号アルゴリズムがRSAアルゴリズムならば、その時にはキー生成ステップは図7に示す通りのものである。KGA152が乱数を要求する最初の時に、CWの値が初期シードとして用いられ、パラメータ「長さ」の値を得るために要求される乱数RNの長さが値128に加算される（これが次期シードの長さになる）。

【0052】次にKGA152は55で動的にシードされる擬似乱数発生器200を呼び出し、「長さ」とシード＝CWを入力パラメータとしてパスする。応答して、動的にシードされる擬似乱数発生器200はCWに等しい入力シードから「長さ」に等しい長さの乱数を生成する。例えば、図12に示すアルゴリズムを動的にシードされる擬似乱数発生器200として用いることができる。「長さ」に等しい長さの生成された乱数RNは56でKGA152にリターンされる。図14は次期シードおよびRNとして56での出力を示す。実際には、生成される乱数RNは（長さ128ビットの）次期シードおよびRN（「長さ」に等しい長さマイナス128ビットの望ましい乱数）の単なる連結である。RNを受理すると、KGA152は次期シードおよびRNを得るためそれをパズする。KGA152が動的にシードされる擬似乱数発生器200に別のコールをすることが必要と判断した場合は、次期シード値はセーブされる。次にRN値がキー生成プロセスで用いられる。次回KGA152が乱数を要求する時に、次期シード値が検索され、シードとして用いられ、また、要求される乱数ランの長さがパラメータ「長さ」の値を得るために値128に加算される。プロセスはこういう風に連続する。もし、キー生成アルゴリズムが図7の方法を用いてRSAキーを生成するならば、図7でステップ161、164、170に入る時には、KGA152は動的にシードされる擬似乱数発生器200にコールする必要がある。必要となる乱

数RN1、RN2等の長さはモジュラスの望みの長さにより、またKGAおよび暗号システム自体の特定の実行によって変る。

【0053】本発明はかかる環境のすべてにおいて、またRSAアルゴリズム、RSAキー生成アルゴリズム、RSA暗号システムの実行において実践できることは当業者は認めるであろう。さらに、これら他のアルゴリズムによるキー生成が、キー生成に含まれるステップがプロセス中のある時点、時期に、動的にシードされる擬似乱数発生器200により生成しうる乱数または無作為値を要求しているという点で、RSAアルゴリズムのキー生成と類似であることを、公用キーアルゴリズムに詳しい人は認めるであろう。このように、本発明はRSAキーの作成のみに限定されず、一般的にパスフレーズから公用キーおよび私用キーを生成する方法が、他の公用キーアルゴリズムに同様に拡張することを当業者は認めるであろう。KGA152がキー生成プロセスを完了後、すなわちPU、PRが生成された後、PUとPRはGPUPR命令52に54でリターンされる。応答して、GPUPR命令52はPU、PRおよび50で入力として供給されたモードおよび制御ベクトルを用いてPUキートークンおよびPRキートークンを構成する。次に既に述べたように、GPUPR命令52は50で入力として供給されたモードおよび制御ベクトルに一貫性チェックを実行し、キータイプおよび使用法がキー生成法に一致しているかどうか（すなわちパスフレーズに基づいているか、パスフレーズに基づいていないか）を判定する。一貫性チェックにパスすれば、PUキートークンとPRキートークンは51でCFAP（キー生成機能）にリターンされる。一方もし、一貫性チェックにパスしないと、GPUPR命令52は停止し、PUキートークンとPRキートークンは51でCFAPにリターンされない。

【0054】パスフレーズ選択プロセス：ユーザにより入力として供給される機密のパスフレーズから、公用キーおよび私用キーペア（PU、PR）を生成するための、本発明の方法を述べてきた。この結果の私用キーPRは入力したパスフレーズの値に完全に依存しており、またキー生成アルゴリズムは公用の知識であると仮定しているので、私用キーPRの機密保護は完全にパスフレーズそのものの機密保護に依存するものと推測される。敵が誰かのパスフレーズの入手または推測することが可能だとしたら、その敵は既知のキー生成アルゴリズムとパスフレーズを用いて私用キーPRを決定できるであろう。ユーザのパスフレーズの機密を保護するのに用いなければならない方策に2つの基本分類がある。即ち：

- ・選択したパスフレーズを無許可のパーティに開示することを防止する方策と、
- ・無許可のパーティが選択したパスフレーズを単純推定することを防止する方策である。

【0055】第1分類の方策は一般にはユーザに原則や指針のセットを提供することにより実行される。例えば、パスフレーズは記憶すべきでメモすべきでない。もしパスフレーズをメモするなら、不慮の開示を避けるため管理された環境の下で行わなければならない。さらにメモしたコピーは不使用时は確実に保管しなければならない。これら規則の大部分は常識そのものであり、システムパスワード、錠の組合せ、私用電話番号の取扱いのような毎日ユーザが扱っている多くの「秘密」に適用されるものである。

【0056】第2分類の方策は常識の原則から明示するのはより困難なことが多い。この方策はユーザがパスフレーズ自体を選択するのに用いる方法に焦点をおく。パスフレーズは他より推定が容易なことは明白である。従って、「良い」パスフレーズ（すなわち容易に推定できないもの）を選択し、「悪い」パスフレーズ（すなわち、容易に推定できるもの）を回避する体系的方法が提供されるべきである。

【0057】図17にパスフレーズ選択プロセスを示す。第1ステップ300は、パスフレーズ選択の原則と指針のセットを準備し発行することである。パスフレーズ選択指針はユーザが「良い」パスフレーズを選択するのを助けるために、ユーザに提供される。これら原則には後章で述べるようにパスフレーズ「フィルタ」を満足するような基準のセットが書面で分かり易い様式で含まれている。

【0058】パスフレーズ選択指針の見本：本章では適切なパスフレーズ作成をユーザに指導するため「べし」と「べからず」のリストを提供する。良い選択と悪い選択とを説明する特定の実施例が与えられる。敵がこの文書を見ていることもあり得るので、実際にはいずれの見本も使用すべきではない。

【0059】基本的にパスフレーズは「構成」しなければならない：敵が推定する恐れのあるレパートリーのフレーズから選択してはならない。さらに、パスワードの構成に当っては語の「数」および語の使用「頻度」は、実用上、敵が大規模、指向性探索を用いてもパスワードを発見できないようなものにする。

【0060】「悪い」パスワード（例えば、自分の名前とか電話番号）を使用すると、無作為に生成されているような見かけを有する暗号キーを作成し、この意味では偶然の侵入者に対してはある程度の保護を与える。しかし、こういったキーは真の暗号保護を与えない。

【0061】避けるべき習慣（過去にこれらを使用して実際に暗号文が解読されたことがある）は次の通りである。

【0062】1. パスフレーズを自分自身で構成する代りに、パスフレーズリスト（例：a book）からパスフレーズを選択しないこと。

【0063】2. フレーズの中の数語が残りの手がかり

りを与えるような推測のできるフレーズを用いないこと。例えば

- ・ よく知られている詩や子守歌からの1行
- ・ よく知られている人、場所、事柄の名前
- ・ 国家、文化、民族、宗教的ヘレディティからのフレーズを使用しないこと。

【0064】3. 以前のパスフレーズと同じ概念のフレーズを使用しないこと。例えば、もし前回、祖父に関することを用いたとしたら、今回は祖母に関することを用いないこと。

【0065】4. パスフレーズとして1語だけというのは使用しないこと。平均的辞書には約10,000語含まれている。この多様性は2の14乗以下であり、電子的速度では直ぐに究明できる。

【0066】5. 最も普通の英語の単語「のみ」を使用しないこと。（すなわち、アングロサクソン起源の基本語）。こうすると敵の辞書のサイズは10,000語以上から、約2,000語またはそれ以下に減らすことができる。

【0067】6. 小学校の教科書にある文を使用しないこと。効力のある習慣は次の通りである。

【0068】1. パスフレーズは新規に創造すること（すなわち、オリジナルであるべきである）

2. パスフレーズの長さはアルファベット文字（A～Z）で空白を除き少くとも40～50文字のこと。これで約10語になり、徹底的なコンピュータ解析を妨げるのに充分である。

【0069】3. 次の1個あるいはそれ以上を行うことにより、敵が必要とするアルファベットまたは辞書を増加させることを考えること。

【0070】・ 特殊記号を含めること（例えば、自分のキーボードにもよるが、||@#\$%「&*()_+-=!@:;,.?"/\|{}<>）

・ 文章に数字を導入すること。

【0071】・ 故意に単語をミススペルすること。

（例：happen 3 stance）

・ 外国語を使用すること。入力記号のセット

を増し、またパスフレーズの各記号は、26可能性の文字の代りに、ずっと多くの可能性の文字数字記号を有することになる。もちろんパスフレーズが記憶困難になるという事実によりこの実施の阻害されることがある。

【0072】4. パスフレーズに固有名前を含んでいても支障ない。

【0073】5. パスフレーズを記憶し易くするよう努め、書き留める必要がないようにすること。逆にフレーズは他の誰かが推定することができなくすべきで、自分だけが知っている内輪の情報を含めることを考えること。

【0074】パスフレーズの例：

悪いパスフレーズの例：

- ・ 「Antidisestablishmentarianism」－単一の辞書語
- ・ 「Dick and Jane see Spot run. Jump Spot jump.」－小学1年の教科書
- ・ 「A bee bit me.」－短かすぎる
- ・ 「George Washington Carrer」－有名人
- ・ 「Mary had a little lamb, its fleece was white as snow.」－有名な詩
- ・ 「Thou shalt have no other gods before Me.」－宗教的ヘリテージ
- ・ 「Four score and seven years ago…」－国家的伝統

良いパスフレーズの例：

- ・ 「I have never lived in Chicago at 278 Lake Shore.」
- ・ 「Why do you believe that fishies don't float in the sky?」
- ・ 「Did George Washington read Pascal or talk to an ambassador?」
- ・ 「My favorite color is green or am I lying & it's Moorish Mist.」
- ・ 「Counting "won, too, tree" is childish (but so what)!」
- ・ 「Cannot I dance on my head? I dunno, perhaps I shall.」

パスフレーズフィルタ：再び図17を参照し、ユーザがステップ301でパスフレーズを一旦選択すると、その選択の良否を判断するために発行されている選択指針に対しユーザ選択を評価することは有益である。この評価プロセスには指針と原則300で発行されているもの以上の追加基準を勿論含むことがある。追加基準を原則の形で述べるのは困難かも知れないが、それにも拘らず選択したパスフレーズの質を判定するには重要である。総合評価基準として、試用パスフレーズを入力し301、試用パスフレーズをテストし302、テスト302の結果を基にして試用パスフレーズを受託または拒否する303、といった具合に自動化することもできる。303で受託されると、順に次のキー生成プロセスの使用可能をトリガする。拒否されるとエラーメッセージをトリガし、ユーザに別のフレーズを選択するよう促す。パスフレーズテスト302はパスフレーズフィルタの形で実行することができる。

【0075】パスフレーズフィルタは「悪い」ユーザ構成のパスフレーズすなわち敵が徹底した指向探索により発見できる可能性のあるパスフレーズを拒否するためのルーチンである。可能性のあるパスフレーズが生成されると、パスフレーズフィルタが呼び出され、パラメータ入力としてパスフレーズが提供される。最も頻繁に使用される10,000語を含む標準英語の辞書を用いて、パスフレーズフィルタは敵のコンピュータプログラムがユーザのパスフレーズを再生成するまでに通常列挙しな

ければならないパスフレーズ数の下限を計算する。この情報は呼び出し者に報告され、パスフレーズの放棄、修正、受託を呼び出し者が選ぶことができる。

【0076】パスフレーズフィルタはそのパスフレーズが「良い」ことを自動的に保証するものではないが、大抵の「悪い」パスフレーズを消去することができる。この意味でパスフレーズ構成用に提供された原則と共にパスフレーズフィルタを用いると、「悪い」パスフレーズが不注意に用いられる機会を最小化し、従って全体の機密保護が向上する。

【0077】パスフレーズフィルタは概念的にはパスワードフィルタと類似しており、「悪い」ユーザ設定のパスフレーズまたは徹底した指向探索により敵が発見できる可能性のあるパスフレーズを拒否するルーチンである。

【0078】パスフレーズを含む例がこのチェック手順の重要性を説明している。ユーザ選定のパスフレーズのような、ユーザ選定のパスワードはよりユーザに親しみやすいアクセス制御とのインタフェースを与える。しかし人間は「容易な道を選ぶ」傾向があることはよく知られている。1000人が選んだ6桁のパスワードを調べてみると、その分布が一樣ではないことは確実である。6個の繰返し数字(000000、111111等)、順番の数字(123456、234567等)または明白なパターンの数字からなるパスワードが不釣合に多いことに気付くであろう。これを知っていると、敵は最もありそうな候補を最初に探索するように徹底した指向探索を組織化できる。多くの場合には、パスワードを見付けるにほんの僅かの試行しか必要としない。対策として、パスワード選択に含まれる潜在的リスクについてユーザに伝えておかなければならないし、またコンピュータシステムの導入においてはパスワード選択において守るべき簡単な原則をセットでユーザに提供しなければならない。弱いパスワードをテストし拒否するために多くのコンピュータシステムではパスワードチェックアルゴリズムを提供することも可能である。

【0079】パスフレーズ構成においては、類似しているが、より複雑な原則のセットを守らなければならない。多くの場合、原則は直観的ではなく、従って、システムに実行されるパスフレーズフィルタは尚更重要である。パスフレーズフィルタは試用パスフレーズに適用される簡単な高速テストのセットからなる。各テストはパスフレーズの変異性を評価する。すべてのテストを実行後、最小値をユーザに報告する。

【0080】図18には、暗号命令セット2を実行可能な暗号化機構し、キー記憶装置3、暗号化機構アクセスプログラム4、ユーザアプリケーションプログラム5よりなる暗号システムを示す。暗号化機構アクセスプログラム4はパスフレーズフィルタユーティリティプログラム6を含み、チェックパスフレーズ7と呼ばれるCFA

Pサービスを通してアクセスされる。試用パスフレーズをチェックするのに次のステップが含まれる。アプリケーション5がチェックパスフレーズサービス7を呼び出す。試用パスフレーズをチェックし、パスフレーズの変異性推定を呼出し者にリターンする。呼出し者は受託のための最小変異性を設定しなければならない。例えばDEAキー生成に対しては、変異性は最小2の56乗であるべきである。

【0081】図19はパスフレーズフィルタルーチンの処理ステップの流れ図である。パスフレーズフィルタは次のチェックを行う。

【0082】1. パターン分析—記号または記号列が繰返されているか？

2. 文字頻度分析—個々の文字、2重字、3重字等が如何なる頻度で典型的な言語では表われ、また提案のパスフレーズに限定するかどうか？

3. ワード頻度分析—特定のワードが如何なる頻度で表われるか？

パスフレーズフィルタによりユーザに報告されるパスフレーズの推定変異性は上記分析のそれぞれから得られる変異性の最小値である。これら分析の実行方法を以下に述べる。

【0083】パターン分析：試用パスフレーズの標準統計分析で次のことが分る。

【0084】1. パスフレーズに用いられた全アルファベット

2. 文字または文字グループの繰返し

このデータから、統計的変異性の計算が容易にできる。例えば、「有効アルファベット」がパスフレーズ中に表われる記号のみで構成されると仮定し、またパスフレーズの「有効長さ」をすべての繰返しを除いたパスフレーズの長さとして定義せよ。そうすると「IIIIII」のようなパスフレーズは「悪い」と分類するであろう。

【0085】数字や文字の自然の順番もある。この自然の順番を用いると、パスフレーズは敵に推測されうかも知れない。数字やアルファベット順を検知する一方法は各数字および文字にランク番号を割り当て、有限差分計算法を用いることである。この方法は有限個数の指定点を通る多項式の次数を計算するのに使われる方法である。この方法を以下に示す。

【0086】1. 数字0～9にランク番号1～10を割り当て、文字「A」～「Z」にランク番号11～36を割り当てる。

【0087】2. パスフレーズに対するランク番号のリストを生成する。

【0088】3. 左端から始めて、各要素から直ぐ右側の要素を減算し、一次差分を計算する。リストの最後の数字はそれに対し計算すべき差分を有しない。

【0089】4. 一次差分の数に同じ操作を行って二次差分を計算する。

【0090】例えば、パスフレーズを次のように仮定し、

パスフレーズ： 1 2 3 4 5

ランク番号： 02 03 04 05 06

一次差分： 01 01 01 01

二次差分： 00 00 00

一次差分のリストにおいて入力がゼロの時は、隣接したランク番号が同一であることを意味する。二次差分のリストにおいて入力がゼロの時は一次差分が同一すなわちランク番号が定数だけ変化していることを意味し、パスフレーズの1片が「246」とか「ABC」のような順序になっていることを意味する。可変性計算では、パスフレーズの有効長さは一次および二次差分リストにあるゼロの数だけ減算される。（このようなゼロは繰返しまたは単純パターンを示すので）。

【0091】このランク番号分析は「qwerty」（または他の）キーボードの数字と文字の順番でもって行うことも可能である。

【0092】文字頻度分析：次の文字リストはGaines（参考文献2）からとったものである。

【0093】英文での文字の頻度順リストは、
ETAONISRHLDCUPFMWYBGVKQXJZ。

【0094】もし特殊記号が含まれるとすれば、その時は最も普通の記号（「E」よりもさらに）はブランクすなわちスペースである。英文での2重字の頻度順リストは

TH HE AN IN ER RE ES ON E
A TI AT STEN ND OR TO NT
ED IS AR…

英文での3重字の頻度順リストは

THE AND THA ENT ION TIO F
OR NDE HASNCE EDT TIS OFT
STH MEN…

1. 各文字を頻度グループにグループ分けして、各グループに変異性の推定値を与える。簡単のため、グループの変異性は2の整数べきであるようにグループを定義する。

【0095】a. 2の0乗 (2⁰) E

b. 2の1乗 (2¹) T

c. 2の2乗 (2²) AO

d. 2の3乗 (2³) NISR

e. 2の4乗 (2⁴) HLDCUPEM

f. 2の5乗 (2⁵) WYBGVKQXJZ

g. ブランク以外の特殊記号には2の5乗の値を付ける。

【0096】2. パスフレーズにおける文字の繰返しパターンをチェックし、分析しようとするパスフレーズから繰返しパターンを取り除く。

【0097】3. 分析しようとするパスフレーズから

すべてのブランクを取り除く。

【0098】4. (パターンを取り去った後の) 各文字に対応する2のべき指数を合計する。合計値がこのテストの変異性である。

【0099】5. 2重字および3重字についても同じことを行う。

【0100】ワード頻度分析：以下はJohn B. Carrollの「The American Heritage WordFrequency Book」(1971)からとったものである。最も普通の英語100ワードの頻度順リストは以下の通りである。

【0101】THE OF AND A TO IN IS YOU THAT IT HE FOR WAS ON ARE AS WITH HIS THEYAT BE THIS FROM I HAVE OR BY ONE HAD NOT BUT WHAT ALL WERE WHEN WE THE RECAN AN YOUR WHICH THEIR SAID IF DO WILL EACH ABOUT HOW UP OUT THEM EHENSHE MANY SOME SO THESE WOULD OTHER INFO HAS MORE HER TWO LIKE HIM SEETIME COULD NO MAKE THAN FIRST BEEN ITS WHO NOW PEOPLE MY MADE OVER DIDDOWN ONLY WAY FIND USE MAY WATER LONG LITTLE VERY AFTER WORDS CALLEDJUST WHERE MOST KNOW
最も頻繁に使われる10,000ワードを含む標準英語の語彙を用い、ユーザのパスフレーズを再生成するまでに敵のコンピュータプログラムが列挙しなければならないであろうパスフレーズ数の下限をユーティリティプログラムが計算する。

【0102】1. 次のようにワード頻度リストを構築する。

- 【0103】a. 2の0乗 (2^{**0}) THE
b. 2の1乗 (2^{**1}) OF
c. 2の2乗 (2^{**2}) AND A
d. 2の3乗 (2^{**3}) TO IN IS YOU
e. 2の4乗 (2^{**4}) THAT IT HE FOR WAS ONARE AS
f. 等々

所望の長さにワード頻度リストに対するこのリストを構築する。あるワードがそのリストに現れなければ、そのリストの最少頻度ワードと同じ頻度を有するものと仮定する。

【0104】2. 繰返しワードをチェックし、分析しようとするパスフレーズから繰返しワードを取り除く。

【0105】3. パスフレーズの各ワードに対応する2のべき指数を合計する。合計値がこのテストの変異性である。

【0106】本発明の特定の実施例を開示したが、本発明の精神および目的から逸脱することなく、特定の実施例に変更を行いうことは当業者には自明である。

【0107】本発明の公用キー暗号システムを管理する方法は、ユーザに知られている第1のシード値を用いて第1の公用キー、私用キーペアを生成し、また第1の公用キー、私用キーペアの第1の使用を定義する第1の制

御ベクトルを生成するステップと、ユーザに知られている第2のシード値を用いて第2の公用キー、私用キーペアを生成し、また第2の公用キー、私用キーペアの第2の使用を定義する第2の制御ベクトルを生成するステップと、第1の制御ベクトルを用いて第1の公用キー、私用キーペアの使用を制御ベクトルするステップと、第2の制御ベクトルを用いて第2の公用キー、私用キーペアの使用を制御ベクトルするステップとを含んでいる。

【0108】ここで、第1のシード値がパスフレーズから生成されてもよく、第2のシード値が真の乱数であってもよい。また、第1のシード値を用いて第1の乱数を生成し、第1の生成ステップに第1の乱数を適用するステップを含んでもよい。さらに、擬似乱数発生器に前記第2のシード値を用いて第2の乱数を生成し、第2の生成ステップに第2の乱数を適用してもよい。

【0109】また、第1の制御ベクトルが2つの構成要素として、第1の公用キーの使用を制御するための第1の公用キー制御ベクトルおよび第1の私用キーの使用を制御するための第1の私用キー制御ベクトルを有してもよい。

【0110】あるいは、第2の制御ベクトルが2つの構成要素として、第2の公用キーの使用を制御するための第2の公用キー制御ベクトルおよび第2の私用キーの使用を制御するための第2の私用キー制御ベクトルを有してもよい。

【0111】第1の制御ベクトルが第1の私用キーを制御してその使用をデジタル署名の生成に制限しまた第2の制御ベクトルが第2の私用キーを制御して、その使用をデジタル署名の生成に制限し、かつキー分散プロトコルの一部として受信した暗号化されたキーを解読してもよい。

【0112】または、第1の制御ベクトルが第1の公用キーの使用をデジタルシグニチャの検証に制限し、また第2の制御ベクトルが第2の公用キーの使用をデジタルシグニチャの検証およびキー分散プロトコルにおけるキーの暗号化に制限してもよい。

【0113】あるいは、第1の制御ベクトルは第1の私用キーによりデジタルシグニチャの生成を制御し、また第2の制御ベクトルは第2の私用キーの使用をデジタルシグニチャの生成には禁止してもよい。

【0114】また本発明の公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法は、ユーザに知られている第1のシードを用いて第1の公用キー、私用キーペアを生成し、また第1の公用キー、私用キーペアの第1の使用を定義する第1の制御ベクトルを生成するステップと、ユーザに知らない第2のシード値を用いて第2の公用キー、私用キーペアを生成し、また第2の公用キー、私用キーペアの第2の私用キーペアを定義する第2の制御ベクトルを生成するステップと、第1の制御ベクトルを用いて第1の公用キー、私用

キーペアの使用を制御するステップと、第2の制御ベクトルにより第2の公用キー、私用キーペアの使用を制御するステップとを含んでいる。

【0115】ここで、第1のシード値がパスフレーズから生成されてもよく、また第2のシード値が真の乱数であってもよい。

【0116】また、第1のシード値を用いて第1の乱数を生成し、また第1の生成ステップに第1の乱数を適用するステップの遂行を含んでもよい。

【0117】あるいは、擬似乱数発生器における第2のシード値を用いて第2の乱数を生成し、また第2の生成ステップに第2の乱数を適用するステップの遂行を含んでもよい。

【0118】第1の制御ベクトルが2つの構成要素として、第1の公用キーの使用を制御するための第1の公用キー制御ベクトルおよび第1の私用キーの使用を制御するための第1の私用キー制御ベクトルを有してもよい。

【0119】第2の制御ベクトルが2つの構成要素として、第2の公用キーを制御するための第2の公用キー制御ベクトルおよび第2の私用キーを制御するための第2の私用キー制御ベクトルを有してもよい。

【0120】第1の制御ベクトルが、第1の私用キーを制御して、その使用をデジタル署名の生成に制限し、また第2の制御が第2の私用キーを制御して、その使用をデジタル署名の生成およびキー分散プロトコルの一部として受信した暗号化されたキーの解読を制限してもよい。

【0121】第1の制御ベクトルが、第1の公用キーの使用をデジタル署名の検証に制限し、また第2制御ベクトルが第2公用キーの使用をデジタル署名の生成およびキー分散プロトコルにおけるキーの暗号化を制限してもよい。

【0122】第1制御ベクトルが第1私用キーでもってデジタル署名の生成を制御ベクトルし、また第2制御ベクトルが第2私用キーの使用がデジタル署名の生成を行うことを禁止してもよい。

【0123】本発明の公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置は、ユーザに知られる第1シード値を用いて第1公用キー、私用キーペアを生成し、また第1公用キー、私用キーペアの第1使用を定義する第1制御ベクトルを生成する第1生成手段と、ユーザに知られない第2シード値を用いて第2公用キー、私用キーペアを生成し、また第2公用キー、私用キーペアの第2使用を定義する第2制御ベクトルを生成する第2生成手段と、第1制御ベクトルを用いて第1公用キー、私用キーペアの使用を制御するための、第1生成手段に連結される制御手段と、第2制御ベクトルにより第2公用キー、私用キーペアの使用を制御するための、第2生成手段に連結される制御手段とを含んでいる。

【0124】ここで、第1シード値がパスフレーズから生成されてもよく、第2シード値が真の乱数であってもよい。

【0125】第1生成手段が、第1シード値を用いて第1乱数を生成し、また第1公用キー、私用キーペアの生成に第1乱数を適用してもよい。

【0126】第2生成手段が、擬似乱数発生器において第2シード値を用いて第2乱数を生成し、また第2公用キー、私用キーペアの生成に第2乱数を適用してもよい。

【0127】第1制御ベクトルが2構成要素として、第1公用キーの使用を制御するための第1公用キー制御ベクトルおよび第1私用キーの使用を制御するための第1私用キー制御ベクトルを有してもよい。

【0128】第2制御ベクトルが2構成要素として、第2公用キーの使用を制御するための第2公用キー制御ベクトルおよび第2私用キーを制御ベクトルするための第2私用キー制御ベクトルを有してもよい。

【0129】第1制御ベクトルが第1私用キーの使用をデジタル署名の生成に制限するよう第1私用キーを制御し、また第2制御ベクトルが第2私用キーの使用をデジタル署名の生成およびキー分散プロトコルの一部として受信される暗号化されたキーの解読に制限するよう第2私用キーを制御してもよい。

【0130】第1制御ベクトルが第1公用キーの使用をデジタル署名の検証に制限し、また第2制御ベクトルが第2公用キーの使用をデジタル署名の検証およびキー分散プロトコルにおけるキーの暗号化を制限してもよい。

【0131】第1制御ベクトルは第1私用キーでもってデジタル署名の生成を制御し、第2制御ベクトルは第2私用キーの使用がデジタル署名の生成を禁止してもよい。

【図面の簡単な説明】

【図1】ユーザ i 、 j が共用する暗号システムAにおいてパスフレーズから公用キーおよび私用キーペア生成を説明するブロック図。

【図2】ユーザ i による暗号システムAおよびBにおいてパスフレーズから公用キーおよび私用キーペア生成を説明するブロック図。

【図3】各々が暗号システムを含む多数のデータ処理装置を含む通信ネットワーク10の説明図。

【図4】暗号システム22の構成を示すブロック図。

【図5】暗号化機構30の構成を示すブロック図。

【図6】暗号化機構30の暗号アルゴリズム144の構成要素のブロック図。

【図7】RSAキー生成に含まれるステップを説明する暗号化機構30のキー生成アルゴリズム151の構成要素のブロック図。

【図8】「真の」乱数発生器180を説明するブロック

図。

【図 9】初期にシードされる擬似乱数発生器 190 を説明するブロック図。

【図 10】動的にシードされる擬似乱数発生器 200 を説明するブロック図。

【図 11】本発明により動的にシードされる擬似乱数発生器 200 を含むように修正された、暗号化機構 30 の暗号アルゴリズム 144 構成要素のブロック図。

【図 12】動的にシードされる擬似乱数発生器の特定例を説明するブロック図。

【図 13】本発明に従って入力パスフレーズから公用キーおよび私用キーペアの生成に含まれるステップを示すブロック図。

【図 14】本発明に従って公用キーおよび私用キーペア生成 (GPUPR) 命令を説明するブロック図。

【図 15】PU キーおよび PR キートークンを説明するブロック図。

【図 16】PU、PR キートークンの制御ベクトル部分を説明するブロック図。

【図 17】パスフレーズ選択プロセスを説明するブロック図。

【図 18】ユーザアプリケーションが提供する試用パスフレーズテストのためパスフレーズフィルタを用いる暗号システムを説明するブロック図。

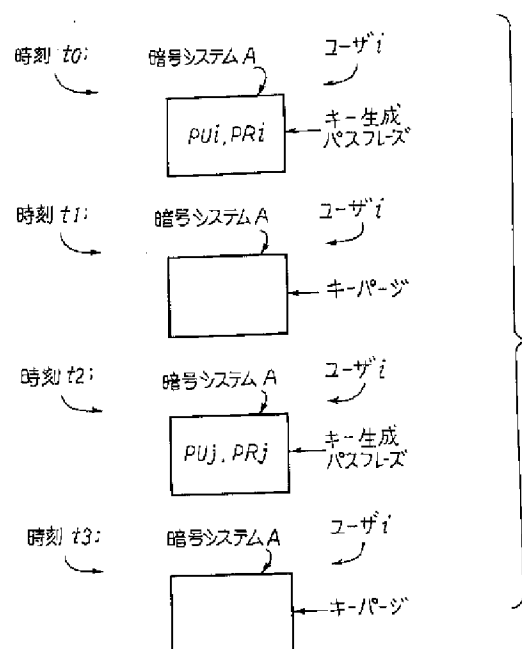
【図 19】パスフレーズフィルタの機能要素を説明するブロック図。

【符号の説明】

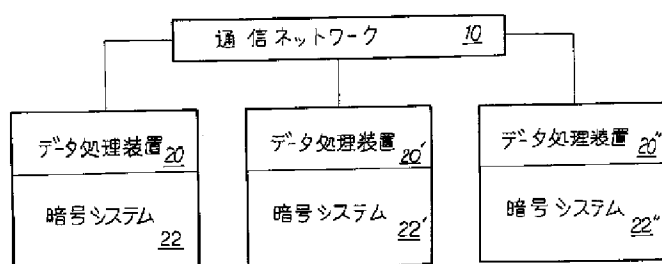
- 1, 30 暗号化機構 (CF)
- 2 暗号命令セット

- 3 キー記憶装置
- 4 暗号化機構アクセスプログラム
- 5 ユーザアプリケーションプログラム
- 6 パスフレーズフィルタユーティリティプログラム
- 7 チェックパスフレーズサービス
- 10 通信ネットワーク
- 20 データ処理装置
- 22 暗号システム
- 32 暗号キーデータセット (CKDS)
- 34 暗号化機構アクセスプログラム (CFAP)
- 36 アプリケーションプログラム (APPL)
- 42 アプリケーションプログラム A (APPL A)
- 43, 44, 45
- 46 キー記憶装置マネージャ
- 47 キー生成機能
- 48 キーパーズ機能
- 52 GPUPR 命令
- 140 機密保護範囲
- 142 命令処理装置
- 144, 150 暗号アルゴリズム
- 146 暗号化機構環境記憶装置
- 151 キー生成アルゴリズム (KGA)
- 152 乱数生成アルゴリズム
- 180 「真」乱数発生器
- 181 ハードウェア回路
- 190 初期にシードされる擬似乱数発生器
- 191, 201 アルゴリズム
- 194 シード記憶装置
- 200 動的にシードされる擬似乱数発生器

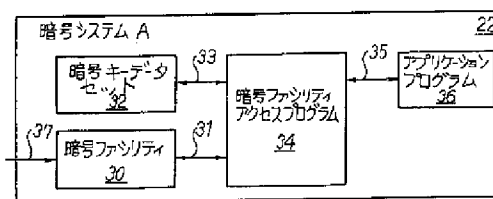
【図 1】



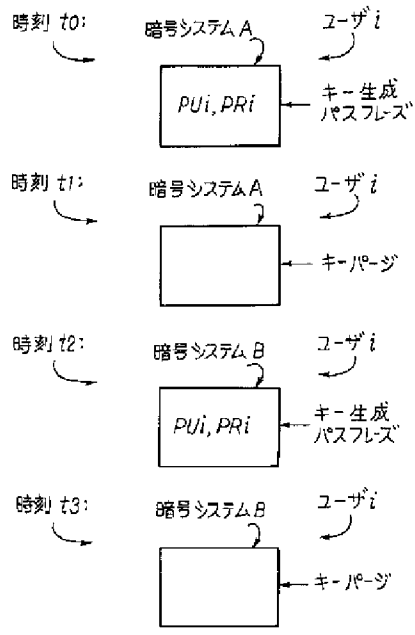
【図 3】



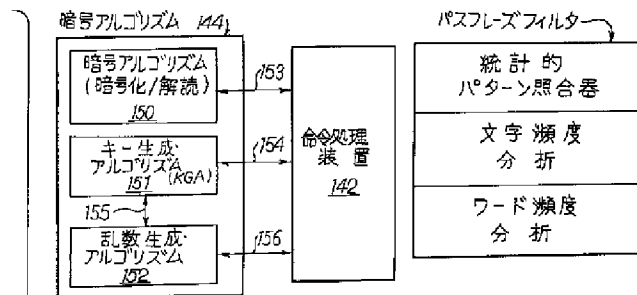
【図 4】



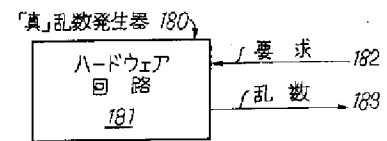
【図 2】



【図 6】

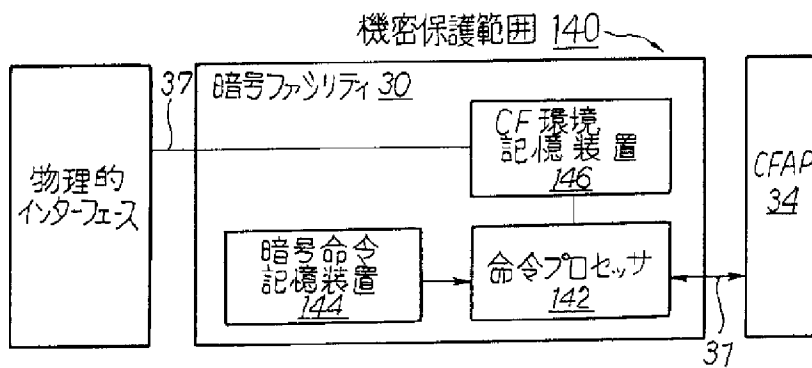


【図 8】



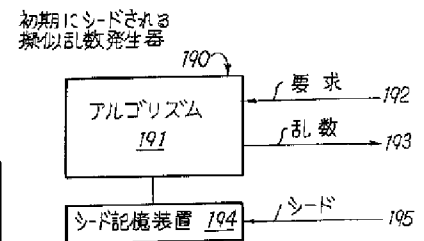
【図 9】

【図 5】

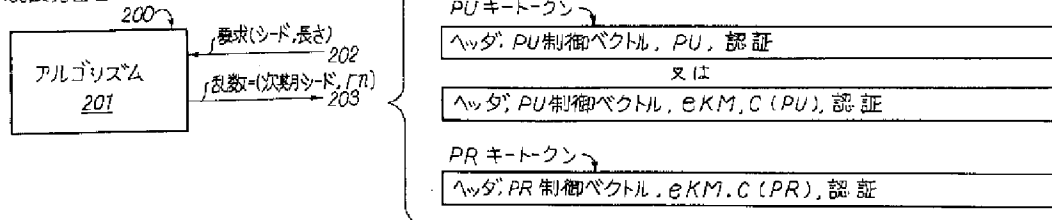


【図 10】

【図 15】

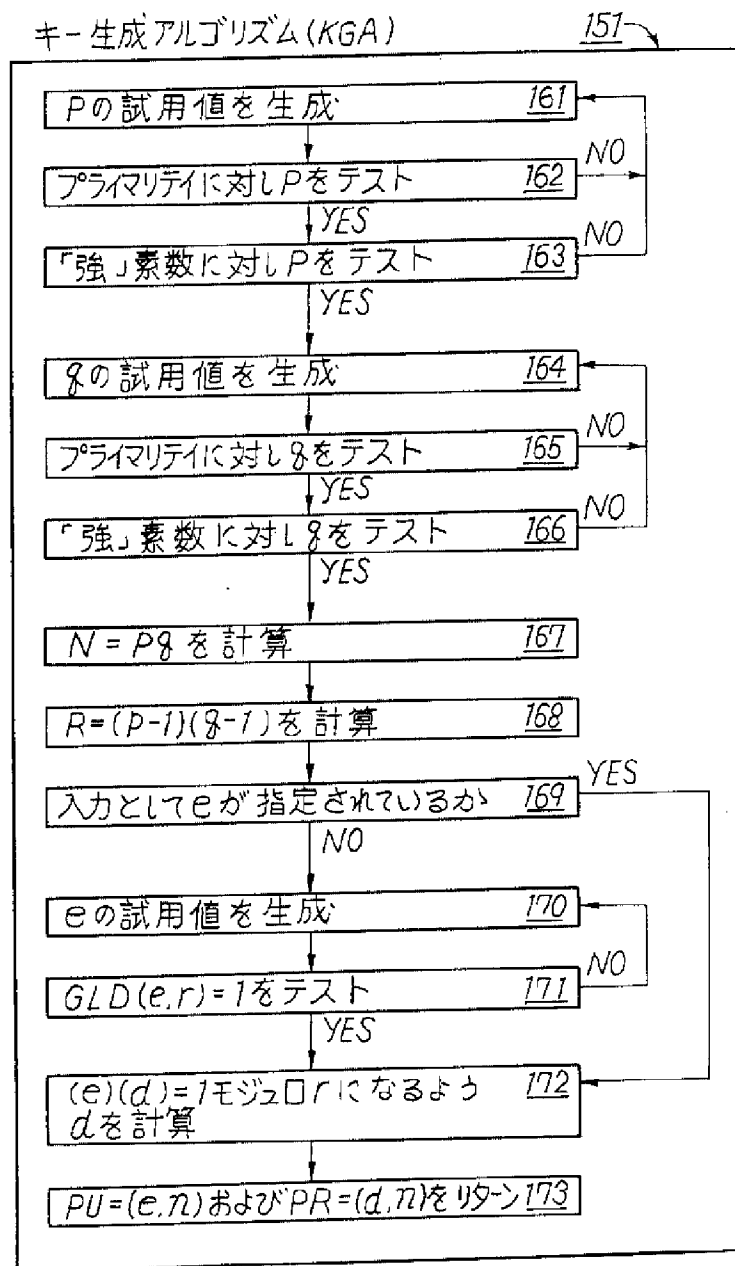


動的にシードされる
疑似乱数発生器

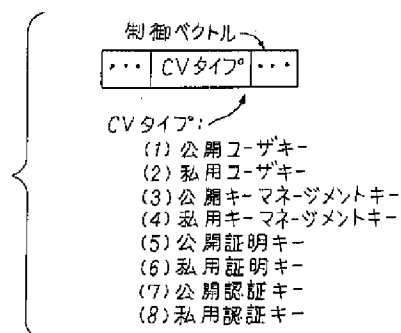
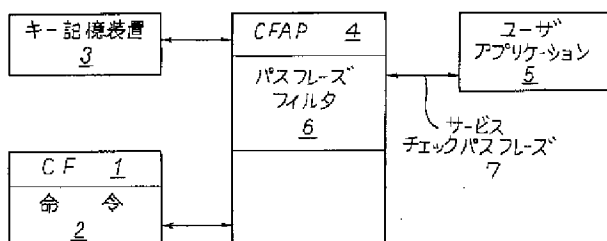


【図7】

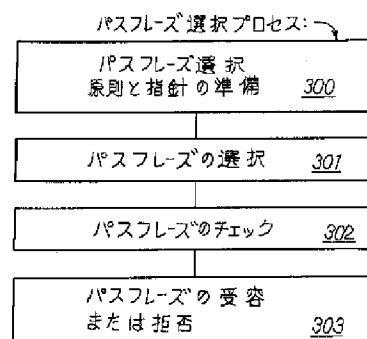
【図16】



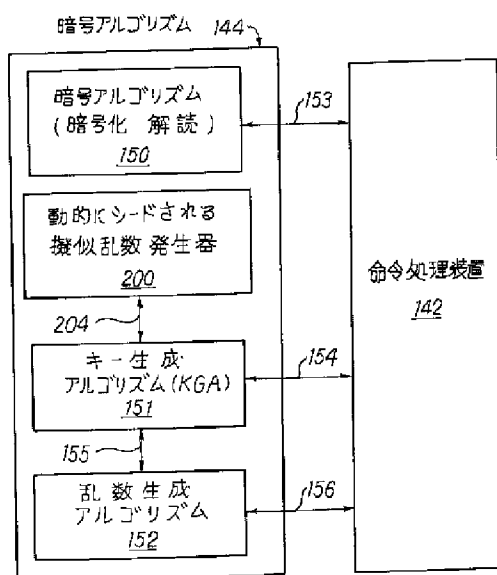
【図18】



【図17】



【図 1 1】



【図 1 2】

動的にシードされる擬似乱数発生器

入 力

m : 生成さるべき乱数の長さをビットで表わす正の整数

シード : 124ビット 値

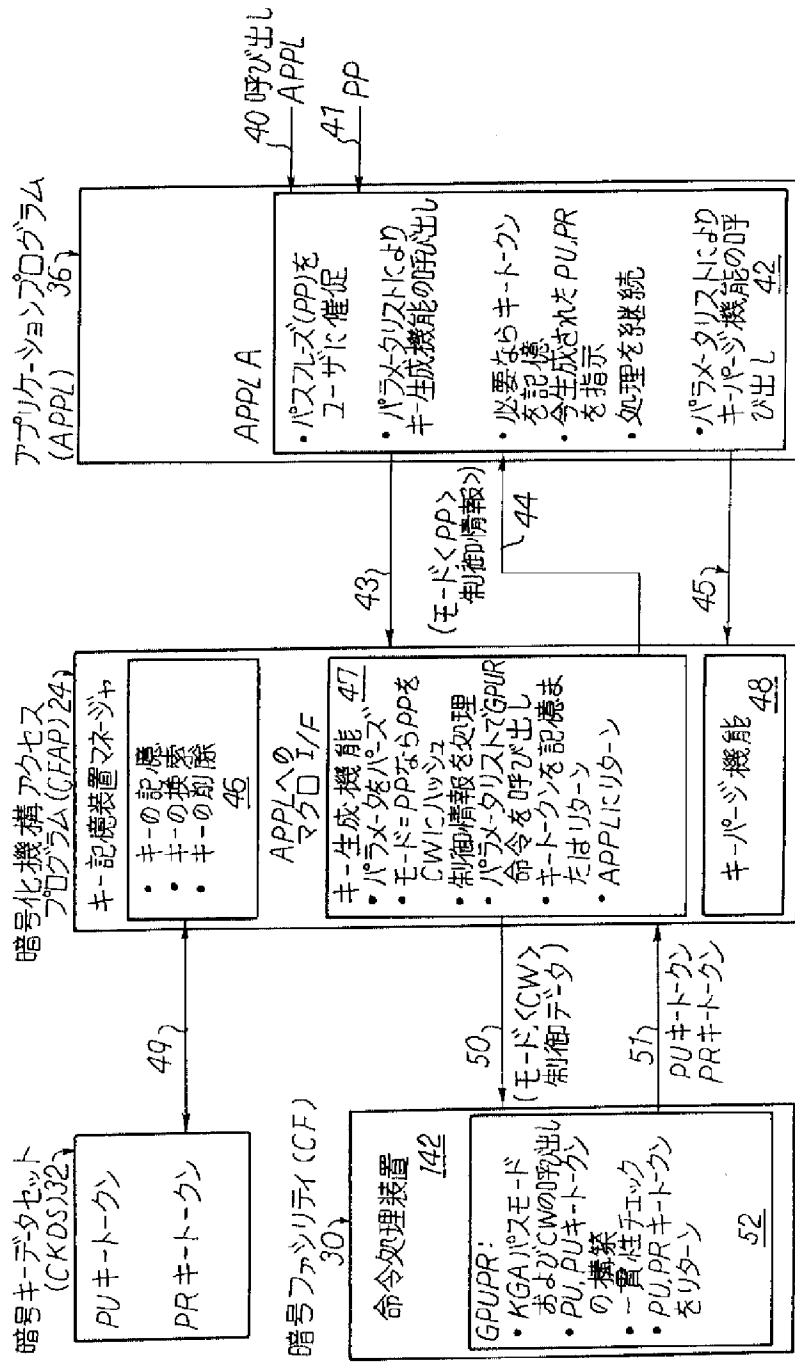
出 力

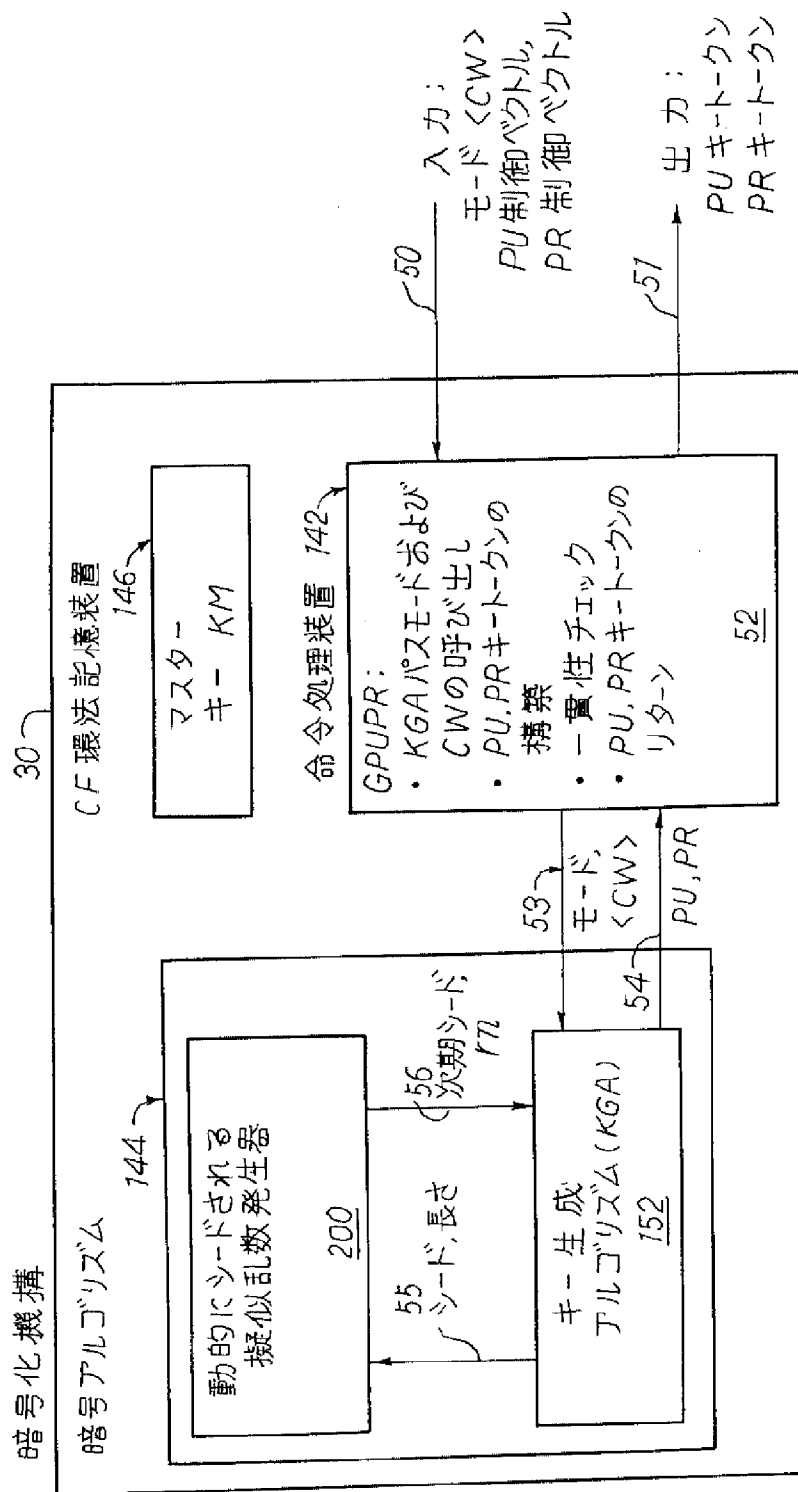
RN : 生成された長さ M ビットの乱数

アルゴリズムの仕様

1. n をセット ; $n = m \div 64$
2. n を次の最大正の整数に丸める
3. K をセット ; K はシードの最も重要な(最左端の)64ビット
4. ICV をセット ; ICV はシードの最も重要でない(最右端の)64ビット
5. A をセット ; A はゼロビットの N ブロック
6. Y をセット ; Y はキーが K , 初期の連鎖値が ICV において、暗号化の暗号ブロック連鎖モードを用い、データ暗号化アルゴリズムにより A を暗号化する時に作成される暗号文
7. RN をセット ; RN は Y の最も重要な(最左端)の m ビット

【図13】





【図14】

【手続補正書】

【提出日】平成4年11月16日

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理する方法であって、ユーザに知られている第1のシード値を用いて第1の公用キー、私用キーペアを生成し、また前記第1の公用キー、私用キーペアの第1の使用を定義する第1の制御ベクトルを生成するステップと、ユーザに知られている第2のシード値を用いて第2の公用キー、私用キーペアを生成し、また前記第2の公用キー、私用キーペアの第2の使用を定義する第2の制御ベクトルを生成するステップと、前記第1の制御ベクトルを用いて前記第1の公用キー、私用キーペアの使用を制御するステップと、前記第2の制御ベクトルを用いて前記第2の公用キー、私用キーペアの使用を制御するステップとを含むことを特徴とする方法。

【請求項2】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理する方法であって、パスフレーズから導出される第1のシード値を用いて第1の乱数を生成するステップと、ユーザには知られない第2のシード値を用いて第2の乱数を生成するステップと、前記第1の乱数を用いて第1の公用キー、私用キーペアを生成し、また前記第1の公用キーおよび前記第1の私用キーの第1の使用を定義するために、それぞれ第1の公用キー制御ベクトルおよび第1の私用キー制御ベクトルを生成するステップと、前記第2の乱数を用いて第2の公用キー、私用キーペアを生成し、また前記第2の公用キーおよび前記第2の私用キーの第2の使用を定義するために、それぞれ第2の公用キー制御ベクトルおよび第2の私用キー制御ベクトルを生成するステップと、前記第1の公用キー制御ベクトルおよび前記第1の私用キー制御ベクトルを用いて、それぞれ前記第1の公用キーおよび前記第1の私用キーの使用を制御するステップと、前記第2の公用キー制御ベクトルおよび前記第2の私用キー制御ベクトルを用いて、それぞれ前記第2の公用キーおよび前記第2の私用キーの使用を制御するステップとを含むことを特徴とする方法。

【請求項3】データ処理システムにおいて、キー発生器

を有する暗号システムを管理する方法であって、パスフレーズから導出される第1のシード値を用いて第1の乱数を生成するステップと、ユーザに知られない第2のシード値を用いて第2の乱数を生成するステップと、前記第1の乱数を用いて第1キーを生成し、また前記第1のキーの使用を制御するための第1の制御ベクトルを生成するステップと、前記第2の乱数を用いて第2のキーを生成し、また前記第2のキーの第2の使用を制御するための第2の制御ベクトルを生成するステップと、前記第1の制御ベクトルにより前記第1のキーの使用を制御するステップと、前記第2の制御ベクトルにより前記第2のキーの使用を制御するステップと、前記第1のキーの前記第1の使用が、前記第2のキーの前記第2の使用と異なるステップとを含むことを特徴とする方法。

【請求項4】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法であって、パスフレーズから導出される第1のシード値を用いて乱数を生成するステップと、前記乱数を用いて公用キー、私用キーペアを生成し、前記第1の制御ベクトルは前記公用キーの使用を制御するもので、前記第2の制御ベクトルは前記私用キーの使用を制御するものであり、前記公用キーに対して前記第1の制御ベクトルを生成し、また前記私用キーに対して前記第2の制御ベクトルを生成するためのステップを含むことを特徴とする方法。

【請求項5】データ処理システムにおいて、公用キー、私用キーペアを含む公用キー暗号システムを管理するための方法であって、パスフレーズから導出されるシード値を用いて乱数を生成するステップと、前記乱数を用いて公用キー、私用キーペアを生成するステップとを含むことを特徴とする方法。

【請求項6】データ処理システムにおいて、公用キー、私用キーペアを含む公用キー暗号システムを管理するための方法であって、パスフレーズから導出される第1のシード値を用いて乱数を生成するステップと、前記乱数を用いて公用キー、私用キーペアを生成し、また前記公用キーに対する第1の制御ベクトルおよび前記私用キーに対する第2の制御ベクトルを生成し、前記第1の制御ベクトルが前記公用キーの使用を制御し、前記第2の制御ベクトルが前記私用キーの使用を制御するステップとを含むことを特徴とする方法。

【請求項7】データ処理システムにおいて、公用キー、

私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
 ユーザに知られる第1シード値を用いて第1公用キー、私用キーペアを生成し、また前記第1公用キー、私用キーペアの第1使用を定義する第1制御ベクトルを生成する第1生成手段と、
 ユーザに知られない第2シード値を用いて第2公用キー、私用キーペアを生成し、また前記第2公用キー、私用キーペアの第2使用を定義する第2制御ベクトルを生成する第2生成手段と、
 前記第1制御ベクトルを用いて前記第1公用キー、私用キーペアの使用を制御するための、前記第1生成手段に連結される制御手段と、
 前記第2制御ベクトルにより前記第2公用キー、私用キーペアの使用を制御するための、前記第2生成手段に連結される前記制御手段とを含むことを特徴とする装置。
 【請求項8】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
 パスフレーズから導出される第1シード値を用いて第1乱数を生成するための第1生成手段と、
 ユーザに知られない第2シード値を用いて第2乱数を生成するための第2生成手段と、
 前記第1乱数を用いて第1公用キー、私用キーペアを生成し、また前記第1公用キーおよび前記第1私用キーの第1使用をそれぞれ定義するための第1公用キー制御ベクトルおよび第1私用キー制御ベクトルを生成する前記第1生成手段と、
 前記第2乱数を用いて第2公用キー、私用キーペアを生成し、また前記第2公用キーおよび前記第2私用キーの第2使用をそれぞれ定義するための第2公用キー制御ベクトルおよび第2私用キー制御ベクトルを生成する前記第2生成手段と、
 前記第1公用キー制御ベクトルおよび前記第1私用キー制御ベクトルをそれぞれ用いて、前記第1公用キーおよび前記第1私用キーの使用を制御するための、前記第1生成手段に連結される制御手段と、
 前記第2公用キー制御ベクトルおよび前記第2私用キー制御ベクトルをそれぞれ用いて、前記第2公用キーおよび前記第2私用キーの使用を制御するための、前記第2

生成手段に連結される制御手段とを含むことを特徴とする装置。

【請求項9】データ処理システムにおいて、キー発生器を有する暗号システムを管理するための装置であって、
 パスフレーズから導出される第1シード値を用いて第1乱数を生成するための第1生成手段と、
 ユーザに知られない第2シード値を用いて第2乱数を生成するための第2生成手段と、
 前記第1乱数を用いて第1キーを生成し、また前記第1キーの使用を制御するための第1制御ベクトルを生成する前記第1生成手段と、
 前記第2乱数を用いて第2キーを生成し、また前記第2キーの第2使用を制御するための第2制御ベクトルを生成する前記第2生成手段と、
 前記第1制御ベクトルでもって前記第1キーの使用を制御するための前記第1生成手段に連結される制御手段と、
 前記第2制御ベクトルでもって前記第2キーの使用を制御するための前記第2生成手段に連結される前記制御手段と、
 前記第1キーの前記第1使用が前記第2キーの前記第2使用と異なることを含むことを特徴とする装置。

【請求項10】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
 パスフレーズから導出される第1シード値を用いて乱数を生成する生成手段と、
 前記乱数を用いて公用キー、私用キーペアを生成し、また前記公用キーに対する第1制御ベクトルおよび前記私用キーに対する第2制御ベクトルを生成し、前記第1制御ベクトルが前記公用キーの使用を制御し、前記第2制御ベクトルが前記私用キーの使用を制御する前記生成手段とを含むことを特徴とする装置。

【請求項11】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
 パスフレーズから導出されるシード値を用いて乱数を生成する生成手段と、
 前記乱数を用いて公用キー、私用キーペアを生成する前記生成手段とを含むことを特徴とする装置。

フロントページの続き

(72)発明者 ドナルド、ビー、ジョンソン
 アメリカ合衆国バージニア州、マナサス、
 クリスタル、クリーク、レーン、11635
 (72)発明者 アン、ブイ、リ
 アメリカ合衆国バージニア州、マナサス、
 バトルフィールド、ドライブ、10227

(72)発明者 ウィリアム、シー、マーティン
 アメリカ合衆国ノースカロライナ州、コン
 コード、ヒリアード、レーン、1835
 (72)発明者 ロスティスロー、プリマク
 アメリカ合衆国バージニア州、ダンフリー
 ズ、フェアウェイ、ドライブ、15900

(72)発明者 ジョン、ディー、ウィルキンズ
アメリカ合衆国バージニア州、サマービ
ル、ピー、オー、ボックス、8